PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-337919
(43)Date of publication of application : 07.12.2001

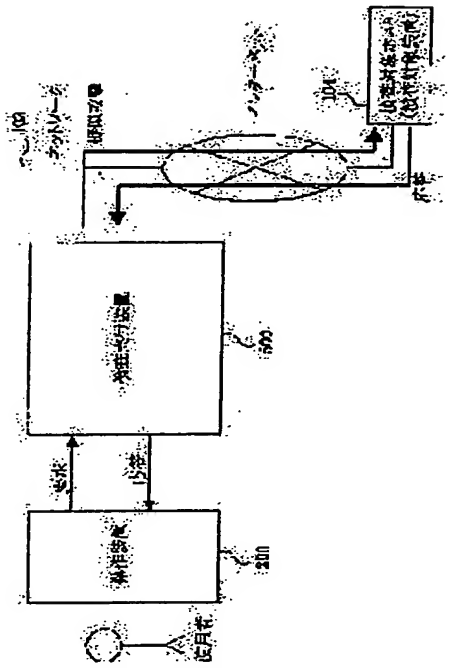
(51)Int.Cl. G06F 15/00
G06F 11/22

(21)Application number : 2000-153601
(22)Date of filing : 24.05.2000

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KAWACHI KIYOTO

(54) SECURITY HOLE DIAGNOSTIC SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide inspection procedures capable of easily implementing an inspection.
SOLUTION: This security hole diagnostic system is provided with an inspection implementing device 500 and an operation device 200. The inspection implementing device 500 is provided with a plurality of inspection implementing means 503 inspecting an inspection object host 104, an inspection implementing means storage section 504 storing a plurality of inspection implementing information defining the information of a plurality of inspection implementing means, and an implementation controller 501 controlling the implementation of a plurality of inspection implementing means and the interface with the operation device 200. The operation device 200 is provided with an operation controller 204 controlling the interface with the inspection implementing device 500 and accepting the instructions inputted from a user, a procedure definition file 202 storing the inspection procedures defining the inspection names indicating the inspections diagnosing a security hole with the inspection implementing means 503 according to the inspection sequence, and a screen generation section 201 displaying an operation screen displaying the inspection names and the names of the inspection implementing means on a display.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The security hole diagnostic method characterized by providing the following. The operating set which receives the directions inputted by the user based on the screen which carries out display ** and is displayed on a display They are two or more inspection activation means by which the above-mentioned inspection activation equipment inspects equipment to be examined in the security hole diagnostic method equipped with the inspection activation equipment which performs inspection to the equipment to be examined which diagnoses a security hole. Two or more inspection execution information which two or more above-mentioned inspection activation means of each are made to correspond, and defines information including the inspection activation means name which shows two or more above-mentioned inspection activation means of each The inspection activation means storing section which matches and stores two or more above-mentioned inspection activation means, It has the execution control section which controls activation of two or more above-mentioned inspection activation means, and controls an interface with the above-mentioned operating set. The above-mentioned operating set The actuation control section which receives the directions which control an interface with the above-mentioned inspection activation equipment, and are inputted by the user, The procedure definition file which memorizes the inspection routine which defines the inspection name which shows inspection which diagnoses a security hole using the above-mentioned inspection activation means according to the sequence to inspect, From the above-mentioned procedure definition file, read inspection routine and it is based on the read inspection routine. The screen generation section acquire inspection execution information from the above-mentioned inspection activation means storing section through the above-mentioned actuation control section, generate the actuation screen which displays an inspection name and an inspection activation means name based on the above-mentioned inspection routine and the acquired inspection execution information, and display the generated actuation screen to the above-mentioned display
[Claim 2] The detailed information corresponding to each is memorized. the inspection name of plurality [file / above-mentioned / procedure definition] as inspection routine, and two or more above-mentioned inspection names -- the above-mentioned screen generation section From the above-mentioned procedure definition file, inspection routine is read and the actuation screen which displays two or more inspection names included in the read inspection routine is generated. The above-mentioned actuation control section The input of the inspection name chosen by the user among two or more inspection names displayed on the actuation screen is received, and the received inspection name is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The security hole diagnostic method according to claim 1 which inputs the above-mentioned inspection name notified from the above-mentioned actuation control section, reads the detailed information corresponding to the inputted inspection name from the above-mentioned inspection routine file, and is characterized by generating the actuation screen which displays the read detailed information.
[Claim 3] The above-mentioned inspection execution information is a security hole diagnostic method according to claim 1 or 2 characterized by for the above-mentioned screen generation section making the inspection name which extracted the inspection name included in the acquired inspection execution information, and was extracted, and a corresponding inspection activation means name correspond, and generating an actuation screen including an inspection name.
[Claim 4] The above-mentioned inspection execution information contains an executable parameter required for activation of an inspection activation means. The above-mentioned actuation screen It matches with the above-mentioned inspection name and an inspection activation means name, and the procedure viewing area to display and the inspection parameter area which displays the above-mentioned executable parameter are included. The

above-mentioned actuation control section The input of the inspection activation means name chosen by the user is received, and the received inspection activation means name is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The inspection activation means name notified from the above-mentioned actuation control section is inputted, and the above-mentioned actuation control section is minded. From the inspection activation means storing section of the above-mentioned inspection activation equipment The inspection execution information corresponding to the inspection activation means which the inputted inspection activation means name shows is acquired. claims 1-3 which extract an executable parameter and are characterized by generating the actuation screen which displays the extracted executable parameter on an inspection parameter area from the acquired inspection execution information — a security hole diagnostic method given in either.

[Claim 5] It is the security hole diagnostic method according to claim 4 which outputs the executable parameter which received the executable parameter into which the above-mentioned actuation control section was inputted by the user including the input area where the above-mentioned inspection parameter area receives the input of an executable parameter, and was received to the above-mentioned execution-control section, and carries out [performing an inspection activation means and] as the description using the executable parameter which the above-mentioned execution-control section inputted the executable parameter from the above-mentioned actuation control section, and inputted.

[Claim 6] Inspection which diagnoses the above-mentioned security hole is performed using two or more inspection activation means. The above-mentioned inspection name It is matched with two or more inspection activation means names. The above-mentioned inspection execution information The run number which shows to what position of two or more inspection activation means used for inspection it performs is included. The above-mentioned screen generation section Two or more inspection execution information containing each is acquired. two or more inspection activation means names matched with the above-mentioned inspection name -- Two or more inspection activation means names and two or more run numbers are extracted from two or more acquired inspection execution information of each. The security hole diagnostic method according to claim 5 characterized by generating the actuation screen which displays the above-mentioned inspection name and two or more extracted inspection activation means names on a procedure viewing area based on two or more extracted run numbers of each.

[Claim 7] The above-mentioned screen generation section is the security hole diagnostic method according to claim 6 which generates the executable parameter contained in two or more inspection execution information of each corresponding to the inspection name performed among the executable parameters which extracted the executable parameter and were extracted as a procedure parameter from two or more acquired inspection execution information of each, and is characterized by to generate the actuation screen which displays the generated procedure parameter on the above-mentioned procedure parameter area.

[Claim 8] The above-mentioned actuation control section receives the input of the inspection activation means name chosen by the user among two or more above-mentioned inspection activation means names. The received inspection activation means name is outputted to the above-mentioned screen generation section. The above-mentioned screen generation section The security hole diagnostic method according to claim 6 which inputs the above-mentioned inspection activation means name, and is characterized by generating the actuation screen which displays the executable parameter corresponding to the inputted inspection activation means name on an inspection parameter area from the above-mentioned actuation control section.

[Claim 9] From equipment to be examined, the above-mentioned execution control section acquires an inspection activation result, and writes the acquired inspection activation result in inspection execution information. The inspection execution information which wrote in the inspection activation result through the above-mentioned execution control section is outputted to the above-mentioned actuation control section. The above-mentioned actuation control section The inspection execution information outputted from the above-mentioned execution control section is inputted, and the inspection activation result included in the inputted inspection execution information is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The security hole diagnostic method according to claim 6 which inputs the notified inspection activation result and is characterized by generating the actuation screen displayed on an inspection parameter area by making the inputted inspection activation result into the above-mentioned executable parameter.

[Claim 10] The above-mentioned execution control section acquires the activation situation of inspection which a security hole diagnoses using an inspection activation means from equipment to be examined. The activation

situation of acquired inspection is outputted to an actuation control section. The above-mentioned actuation control section The activation situation of inspection outputted from the above-mentioned execution control section is inputted, and the activation situation of inspection of having inputted is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The security hole diagnostic method according to claim 1 which acquires the activation situation of inspection notified from the above-mentioned actuation control section, generates the inspection result display screen which displays the acquired activation situation of inspection, and is characterized by displaying the generated inspection result display screen on the above-mentioned display.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the system which diagnoses the existence of the security hole of a computer.
[0002]
[Description of the Prior Art] Conventionally, it is Internet as a diagnostic tool of a comprehensive security hole. Security Internet of Systems It is free and Scanner and nessus currently exhibited are mentioned. These have the database of a known security hole and have the function to inspect the existence of a security hole from the exterior to a host to be examined.
[0003] It is [nmap and] John as a tool which inspects a security hole by actually attacking on the other hand. the The tool called ripper exists. nmap is a tool for specifying the service which is working on a candidate host, and is John. the ripper is a tool which detects the account which had a password brittle as an input for the password file.
[0004]
[Problem(s) to be Solved by the Invention] However, it is only that the above comprehensive security hole diagnostic tools check existence of the security hole of a host to be examined, and what kind of unlawful access does not judge by the possible furnace further using the security hole. Therefore, even if the manager discovered the security hole on the computer put under management using the above-mentioned tool, to what extent it may have been invaded in the past had the trouble that it had to depend on a manager's knowledge and experience.
[0005] as mentioned above, it may be invaded to what extent -- becoming an effective attack, if the existing attack tool is only what realized the single function and they are used in what kind of procedure although that inspection actually needs to attack -- moreover, how the information acquired with a certain tool should be applied with other tools had the large part depending on a user's workmanship.
[0006] This invention is the integrative security hole diagnostic tool which made it possible to be made in order to cancel the above-mentioned trouble, to prepare two or more inspection of a single function, to classify them according to the inspection routine considered to be effective with it being general, and to reuse each inspection result automatically to other inspection.
[0007]
[Means for Solving the Problem] The security hole diagnostic method concerning this invention The operating set which receives the directions inputted by the user based on the screen which carries out display ** and is displayed on a display, In the security hole diagnostic method equipped with the inspection activation equipment which performs inspection to the equipment to be examined which diagnoses a security hole the above-mentioned inspection activation equipment Two or more inspection execution information which two or more above-mentioned inspection activation means of each are made to correspond, and defines information including the inspection activation means name which shows two or more inspection activation means to inspect equipment to be examined, and two or more above-mentioned inspection activation means of each, The inspection activation means storing section which matches and stores two or more above-mentioned inspection activation means, It has the execution control section which controls activation of two or more above-mentioned inspection activation means, and controls an interface with the above-mentioned operating set. The above-mentioned operating set The actuation control section which receives the directions which control an interface with the above-mentioned inspection activation equipment, and are inputted by the user, The

procedure definition file which memorizes the inspection routine which defines the inspection name which shows inspection which diagnoses a security hole using the above-mentioned inspection activation means according to the sequence to inspect, From the above-mentioned procedure definition file, read inspection routine and it is based on the read inspection routine. Inspection execution information is acquired from the above-mentioned inspection activation means storing section through the above-mentioned actuation control section. Based on the above-mentioned inspection routine and the acquired inspection execution information, the actuation screen which displays an inspection name and an inspection activation means name is generated, and it is characterized by having the screen generation section which displays the generated actuation screen on the above-mentioned display.

[0008] The detailed information corresponding to each is memorized. the inspection name of plurality [file / above-mentioned / procedure definition] as inspection routine, and two or more above-mentioned inspection names -- the above-mentioned screen generation section From the above-mentioned procedure definition file, inspection routine is read and the actuation screen which displays two or more inspection names included in the read inspection routine is generated. The above-mentioned actuation control section The input of the inspection name chosen by the user among two or more inspection names displayed on the actuation screen is received, and the received inspection name is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The above-mentioned inspection name notified from the above-mentioned actuation control section is inputted, and the detailed information corresponding to the inputted inspection name is read from the above-mentioned inspection routine file, and it is characterized by generating the actuation screen which displays the read detailed information.

[0009] It is characterized by for the above-mentioned inspection execution information making the inspection name which the above-mentioned screen generation section extracted the inspection name included in the acquired inspection execution information, and was extracted including the inspection name, and a corresponding inspection activation means name correspond, and generating an actuation screen.

[0010] The above-mentioned inspection execution information contains an executable parameter required for activation of an inspection activation means. The above-mentioned actuation screen It matches with the above-mentioned inspection name and an inspection activation means name, and the procedure viewing area to display and the inspection parameter area which displays the above-mentioned executable parameter are included. The above-mentioned actuation control section The input of the inspection activation means name chosen by the user is received, and the received inspection activation means name is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The inspection activation means name notified from the above-mentioned actuation control section is inputted, and the above-mentioned actuation control section is minded. From the inspection activation means storing section of the above-mentioned inspection activation equipment The inspection execution information corresponding to the inspection activation means which the inputted inspection activation means name shows is acquired, and from the acquired inspection execution information, an executable parameter is extracted and it is characterized by generating the actuation screen which displays the extracted executable parameter on an inspection parameter area.

[0011] Including the input area where the above-mentioned inspection parameter area receives the input of an executable parameter, the executable parameter into which the above-mentioned actuation control section was inputted by the user is received, and the received executable parameter is outputted to the above-mentioned execution control section, and it carries out [that the above-mentioned execution control section performs an inspection activation means using the executable parameter which inputted and inputted the executable parameter from the above-mentioned actuation control section, and] as the description.

[0012] Inspection which diagnoses the above-mentioned security hole is performed using two or more inspection activation means. The above-mentioned inspection name It is matched with two or more inspection activation means names. The above-mentioned inspection execution information The run number which shows to what position of two or more inspection activation means used for inspection it performs is included. The above-mentioned screen generation section Two or more inspection execution information containing each is acquired. two or more inspection activation means names matched with the above-mentioned inspection name — From two or more acquired inspection execution information of each, two or more inspection activation means names and two or more run numbers are extracted, and it is characterized by generating the actuation screen which displays two or more inspection activation means names extracted with the above-mentioned inspection name based on two or more extracted run numbers of each on a procedure viewing area.

[0013] The above-mentioned screen generation section generates the executable parameter contained in two or

more inspection execution information of each corresponding to the inspection name performed among the executable parameters which extracted the executable parameter and were extracted as a procedure parameter from two or more acquired inspection execution information of each, and is characterized by generating the actuation screen which displays the generated procedure parameter on the above-mentioned procedure parameter area.

[0014] The above-mentioned actuation control section receives the input of the inspection activation means name chosen by the user among two or more above-mentioned inspection activation means names. The received inspection activation means name is outputted to the above-mentioned screen generation section, and the above-mentioned screen generation section carries out generating the actuation screen which displays the executable parameter corresponding to the inspection activation means name which inputted and inputted the above-mentioned inspection activation means name on an inspection parameter area from the above-mentioned actuation control section as the description.

[0015] From equipment to be examined, the above-mentioned execution control section acquires an inspection activation result, and writes the acquired inspection activation result in inspection execution information. The inspection execution information which wrote in the inspection activation result through the above-mentioned execution control section is outputted to the above-mentioned actuation control section. The above-mentioned actuation control section The inspection execution information outputted from the above-mentioned execution control section is inputted, and the inspection activation result included in the inputted inspection execution information is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The notified inspection activation result is inputted and it is characterized by generating the actuation screen displayed on an inspection parameter area by making the inputted inspection activation result into the above-mentioned executable parameter.

[0016] The above-mentioned execution control section acquires the activation situation of inspection which a security hole diagnoses using an inspection activation means from equipment to be examined. The activation situation of acquired inspection is outputted to an actuation control section. The above-mentioned actuation control section The activation situation of inspection outputted from the above-mentioned execution control section is inputted, and the activation situation of inspection of having inputted is notified to the above-mentioned screen generation section. The above-mentioned screen generation section The activation situation of inspection notified from the above-mentioned actuation control section is acquired, and the inspection result display screen which displays the acquired activation situation of inspection is generated, and it is characterized by displaying the generated inspection result display screen on the above-mentioned display.

[0017]

[Embodiment of the Invention] Actuation of the gestalt of this operation is described below gestalt 1. of operation, referring to drawing. First, system-wide actuation is explained, referring to drawing 1 . This system is delivering a false attack through a network 103 to the host 104 to be examined, and detects the security hole which exists in the host (equipment to be examined) 104 to be examined.

[0018] This system consists of an operating set 200 and inspection activation equipment 500, and the activation result of inspection by which an inspection demand is returned to a user by inspection activation equipment 500 from delivery and inspection activation equipment 500 through an operating set 200 is displayed on an operating set 200.

[0019] Next, an example of the configuration of inspection activation equipment 500 is explained, referring to drawing 2 . Inspection activation equipment 500 consists of the execution control section 501, the candidate host information storing section 502, an inspection activation means 503, and the inspection activation means storing section 504.

[0020] The execution control section 501 controls the inspection activation equipment 500 whole according to the demand from an operating set 200. Each false attack is mounted on the inspection activation means 503. The inspection activation means 503 is stored in the inspection activation means storing section 504. If needed, the inspection activation means 503 is loaded by the execution control section 501 on memory, and delivers a false attack by it.

[0021] The candidate host information storing section 502 is for enabling it to use as information at the time of storing the information about the host 104 to be examined obtained from the false attack, and delivering another false attack from an operating set 200. If an example is given, the IP address of a host to be examined is stored from an operating set 200, or port information on the candidate host acquired by the port scan false attack is stored. They are referred by another inspection activation means.

[0022] Moreover, the inspection activation means storing section 504 is combined, and stores the information corresponding to an inspection activation means as information on an inspection activation means (inspection execution information) while it stores two or more inspection activation means 503. The information on an inspection activation means may be recorded on the interior of the inspection activation means 503.
[0023] The information on an inspection activation means is matched with the inspection activation means 503, and should just be stored in the above-mentioned inspection activation means storing section. Therefore, even when recorded on the interior of the inspection activation means 503, the case where it exists as a separate file is sufficient. The following explanation explains the case where the information on an inspection activation means is recorded on the interior of the inspection activation means 503.
[0024] Next, an operating set 200 is explained, referring to drawing 3 . An operating set 200 is equipped with the screen generation section 201, the procedure definition file 202, the display name definition file 203, the actuation control section 204, and a display 205. The actuation control section 204 controls an interface with inspection activation equipment, and receives the directions inputted by the user. In addition, the actuation control section 204 controls the operating set 200 whole. The procedure definition file 202 is defined according to the sequence of inspecting the inspection routine of a security hole diagnosis.
[0025] The actuation screen which displays inspection routine as the information on the inspection activation means which acquired and acquired the information inspection execution information (inspection execution information) of the inspection activation means storing section 504 to an inspection-routine means based on inspection routine generates through an actuation control section 204 from a procedure definition file 202 based on the inspection routine which read inspection routine and read, and the screen generation section 201 displays the actuation screen generated to the above-mentioned display 205.
[0026] An operating set 200 provides a user with an actuation means with an actuation screen. The actuation screen control section 204 reads the procedure definition file 202 and the display name definition file 203 at the time of starting, and performs required initialization at it.
[0027] The procedure definition file 202 describes the Ruhr for classifying an inspection activation means for the extra information (an execution condition, detail explanation) of a routine name and a procedure, and each procedure, and defines general attack procedures, such as "port scan" and "file acquisition", as them as inspection routine ("inspection routine" is also hereafter called "procedure"). At the time of operating set starting, the inspection activation means belonging to each inspection routine is searched and sorted, and is displayed on a screen. Drawing 4 shows an example of the format of the procedure definition file 202 of the gestalt of this operation.
[0028] The display name definition file 203 is a dictionary for changing into the word of each country the character string displayed on a screen. Drawing 5 shows an example of the format of the display name definition file 203 of the gestalt of this operation.
[0029] An example of an actuation screen is shown in drawing 8 from drawing 6 . Drawing 6 shows an example of the main screen (actuation screen) 301. The main screen 301 is equipped with the procedure viewing area 401 which displays inspection routine, and the inspection parameter area 402 used with the inspection activation means 503. Drawing 7 shows an example of the candidate host information input screen 302. Drawing 8 shows an example of the inspection result display screen 303.
[0030] The procedure viewing area 401 displays the "inspection routine" which can be performed by this system as a node of a tree, and displays the inspection activation means name corresponding to ** "inspection routine" as the subnode further.
[0031] The inspection parameter area 402 is generated corresponding to the "inspection routine" or the inspection activation means name chosen on the procedure viewing area 401, and displays the screen for inputting a parameter required in order to perform the selected procedure or inspection.
[0032] Display and elimination of these actuation screens are done if needed. The candidate host information input screen 302 is a screen for performing display and edit of the information stored in the candidate host information storing section 502 in inspection activation equipment 500. A user specifies the equipment inspected using the candidate host information input screen 302. The inspection result display screen 303 is a screen which displays the activation result of inspection.
[0033] The operating instructions of this operating set 200 are described briefly. A user's starting of an operating set 200 displays the main screen 301 shown in drawing 6 . The node (procedure node) showing inspection routine of inspection routine is displayed on the procedure viewing area 401. Moreover, the inspection activation means name (node of an inspection activation means) classified into each procedure is displayed as

the subnode.
[0034] The parameter input screen where he corresponded when the user chose the node (procedure node) of inspection routine or the node of an inspection activation means is generated on the inspection parameter area 402. This expresses the input item of the execution-time parameter which a user has to give, in order to perform inspection corresponding to the selected node. When a procedure node is chosen, all parameters required in order to perform all the inspection activation means 503 classified into the inspection routine are displayed.
[0035] Only it is performed when it inspects, where the node of an inspection activation means is chosen. Where a procedure node is chosen, when it inspects, an inspection activation means to belong to the selected procedure node as a subnode is performed in order. An activation result can be checked in the inspection result display screen 303.
[0036] the case where it inspects by choosing a procedure node -- the property top of the inspection routine -- "-- even [either] -- also coming out --" thing which should be just successful, and what "it is better to perform all" can be considered. For example, if at least one procedure of an inspection activation means to connote of "file acquisition" is successful, the purpose can be attained, but in the case of "port scan", a result can be maximized when all inspection activation means to connote are performed.
[0037] When a procedure node is chosen, he is trying to express the radio button for activation terminating condition selection as the gestalt of this operation on the inspection parameter area 402, in order that a user may enable it to control these. A radio button can be chosen from three kinds, "it is an inquiry to a user". ["ending, when it succeeds"; "performing all", and] A user chooses [above-mentioned] one from three kinds.
[0038] Drawing 9 is drawing showing the method of presentation of the running state of the inspection activation means in an actuation screen. A user is notified of the activation situation of inspection by displaying the icon expressed with drawing 9 on the node in the corresponding procedure viewing area 401.
[0039] As a result of inspection, a "password file" may be able to be acquired or account and a password may become clear. Next, when the inspection routine which needs them as an input parameter, or an inspection activation means is chosen, the they-acquired data are set to GUI for parameter inputs in the inspection parameter area 402 as a default.
[0040] Next, actuation of this system is explained. First, the processing at the time of starting is explained, referring to drawing 10 , drawing 11 , and drawing 12 . The processing at the time of starting is roughly classified into three. They are an information reading phase, a procedure parameter generation phase, and a screen-display phase.
[0041] Drawing 10 is a flow chart which shows the classification procedure (information reading phase) of the inspection activation means in an actuation screen. Drawing 11 is a flow chart which shows the initialization procedure (procedure parameter generation phase) of the inspection routine information at the time of initialization. Drawing 12 is a flow chart which shows the initial-screen construction procedure (screen-display phase) in the procedure viewing area 401 in an actuation screen. Hereafter, order is explained later on.
[0042] Drawing 10 is a flow chart showing an information reading phase. A system reads the procedure definition file 202 by 801 at the time of a system startup. The procedure definition file is carrying out the format as shown by drawing 4 , and consists of a sort key name and a list of procedure definition entries (a key value, a category name (procedure display name), an activation terminating condition, detail explanation).
[0043] By drawing 4 , the sort key name shows PLUGIN_TYPE as an example. Moreover, the procedure definition entry is described by the format of <key value> = <category name (procedure display name)> ¥<activation terminating condition >¥ <detail explanation> in drawing 4 .
[0044] An example of the configuration of a procedure definition file is shown in drawing 13 . The procedure definition entry expressed as the sort key name as "key value = classification place category information" is included in a procedure definition file as mentioned above. The parts of a category name (procedure display name), an activation terminating condition, and detail explanation of classification place category information correspond.
[0045] The operation of a category name, an activation terminating condition, and detail explanation is shown in drawing 13 .
[0046] Next, the procedure data dictionary (Map) which can be searched with a key value is generated from the read list of procedure definition entries by 802. The data stored in Map are the structure with the element of (a procedure display name (category name), an activation terminating condition, procedure explanation (detail explanation of a procedure definition entry), the list of inspection activation means information, and a procedure parameter). The list and procedure parameter of inspection activation means information are empty in this

phase.
[0047] By 803-809, the information on all the inspection activation means 503 to the inspection activation means stored in the inspection activation means storing section 504 of inspection activation equipment 500 is acquired. The information on the acquired inspection activation means searches a sort key name as a property name, and acquires a key value as a searched result. Map is searched with the acquired key value and it registers with the list of the inspection activation means information in the corresponding procedure data.
[0048] First, the screen generation section 201 reads a procedure definition file, and acquires a sort key name (for example, the procedure definition file of drawing 4 "PLUGIN_TYPE"). Next, the screen generation section 201 reads the inspection activation means 503 stored in the inspection activation means storing section 504 of inspection activation equipment 500 through the actuation control section 204, and acquires the information on an inspection activation means. Relation with the information on the inspection activation means 503 and an inspection activation means is shown in drawing 14 .
[0049] Next, the screen generation section 201 acquires the value of the data applicable to a sort key name (here "PLUGIN_TYPE") from the information on the acquired inspection activation means. Signs that the value of data is acquired to drawing 15 are shown. Here, the value of the acquired data supports the key value in the procedure definition file 202.
[0050] Based on the taken-out value (here "PASSWORD_CRACK"), the classification place category which corresponds within the procedure definition file 202 is searched. An inspection activation means node is generated as a child node of the node on the screen corresponding to the corresponding classification place category. The activation inspection name ("NAME") property (in the case of drawing 15 , it is "john") of the information on an inspection activation means is used for the identifier of the node to generate.
[0051] It carries out about all inspection activation means by which the process of 2-5 is saved.
[0052] The information on an inspection activation means is the list of the data which make a property name, data type, and a value one entry, as shown in drawing 15 . Two or more these lists exist. It is possible to make a list nest a value further. The information on an inspection activation means contains two properties, an activation inspection name (a property name is "NAME") (string type) and an activation parameter list (a property name is "PARAMETER") (list-directed), at least.
[0053] The attribute of others which are contained in the information on an inspection activation means can be added to arbitration for every inspection activation means. Each attribute is identified by the property name. The information on an inspection activation means contains the run number which shows whether it is an inspection activation means to perform to what position among two or more inspection activation means to correspond to the key value of 1.
[0054] Drawing 16 shows an example of the activation parameter list contained in the information on an inspection activation means. The part applicable to the activation parameter list of the information on an inspection activation means makes a property name "PARAMETER". An activation parameter list is a list of the data which make a parameter name, data type, and a default one entry.
[0055] An executable parameter specifies the parameter which must be given to an inspection activation means, when performing an inspection activation means. A default is a value used when a parameter should carry out and it carries out. Moreover, when there is a value of a parameter except tolerance or errors of a parameter, such as an insufficient ****** case, occur [a parameter], the message which warns a user of an error is displayed at the time of inspection activation, and the input of a parameter is urged to it. The activation parameter list in the information on the above-mentioned inspection activation means is a list of the data which make a parameter name, data type, and a default one entry.
[0056] Next, processing of a procedure parameter generation phase is explained, referring to drawing 11 . The purpose of this phase is generating a parameter list which connotes all the activation parameter lists contained in the inspection activation means information belonging to ** "inspection routine", and registering it as a procedure parameter in procedure data.
[0057] The flow chart expressed with drawing 11 consists of two nested loop formations. One is a loop formation expressed with 1002-1011, and this means that 1003-1009 are performed over all the procedure data in Map. Another is a loop formation expressed with 1006-1009, and this means that 1007-1008 are performed over all the inspection activation means information registered into the inspection activation means information list of [in each procedure data].
[0058] All the activation parameter lists acquired by 1007 are compounded by 1008, and the final result is 1010 and they are registered as a procedure parameter in procedure data. The intermediate result Pt and the

activation parameter list (param_list) acquired by 1007 are compared with the composition carried out by 1008, and when an entry with the parameter name which does not exist in Pt exists in param_list, it realizes by adding the entry to Pt.

[0059] The procedure parameter generated by the above-mentioned processing expresses the parameter list indispensable to perform all the inspection activation means included in the "inspection routine."

[0060] Next, processing of a screen-display phase is explained, referring to drawing 12 . The flow chart expressed with drawing 12 consists of two nested loop formations. An outside loop formation is a loop formation expressed with 1102-1111. Over all the procedure data in Map, this generates a node on the procedure viewing area 401, further, is executing loop formations 1106-1110 in the interior, and generates the node corresponding to the inspection activation means registered into each procedure data as a subnode of a procedure node. The information on procedure data or an inspection activation means is related with each generated node. The above is explanation about the processing at the time of this system startup.

[0061] Next, generation processing of the inspection parameter area 402 when a user clicks the node on the procedure viewing area 401 is explained. Drawing 17 and drawing 18 are the flow charts showing generation processing of the inspection parameter area 402 at the time of clicking the node (procedure node) to which a user expresses the inspection routine on the procedure viewing area 401. All the contents currently displayed by then are eliminated in a procedure 1201. Next, it acquires based on the node which had the procedure data D ("the procedure data D" is hereafter called "D") related with the node by the screen generation phase of processing in the first half at the time of starting clicked (procedure 1202). Next, detail explanation is taken out from D and it displays on the inspection parameter area 402 (procedure 1203).

[0062] Next, the radio button with which an activation terminating condition is expressed on a screen is generated, and the radio button corresponding to the activation terminating condition registered by D is changed into a selection condition (procedure 1204). the gestalt of this operation -- as an activation terminating condition -- "-- even -- also coming out -- if it succeeds -- termination" and "performing all" -- "-- if it succeeds, three kinds of inquiry" will be prepared for the user.

[0063] Next, the procedure parameter list P ("the procedure parameter list P" is hereafter called "P") is acquired from D (procedure 1205), and the input screen which corresponds by loop formations 1207-1215 is displayed on the inspection parameter area 402 to each parameter entry in P.

[0064] By loop formations 1207-1215, it processes as follows. The i-th element of P will be expressed as P [i]. First, a parameter name is acquired from P [i] in a procedure 1208, and it displays on the inspection parameter area 402. At this time, a display name is changed into intelligible language according to the contents of the display name definition file 203 read at the time of starting. Next, the data type of P [i] is estimated by the procedure 1209, and processing branches by the result.

[0065] When data type is a character string or a numeric value, a text box is displayed on the bottom of the parameter name which displayed the point (procedure 1210). The default set as P [i] is displayed on a text box (procedure 1211).

[0066] When data type is binary, the text box which inputs the pathname of the file by which binary data were stored under the parameter name is displayed (procedure 1212). Next, "reference" carbon button which displays the dialog for choosing the file in which binary data are stored beside the parameter name is generated (procedure 1213). Finally, a default is taken out from P [i] and it sets to a text box (procedure 1214).

[0067] An example of the screen generated by the above processing is the inspection parameter area 402 in drawing 19 . Drawing 19 also shows the source of the data currently displayed.

[0068] Drawing 20 and drawing 21 are the flow charts showing generation processing of the inspection parameter area 402 at the time of clicking the node (node of an inspection activation means) to which a user expresses the inspection activation means on the procedure viewing area 401. All the contents currently displayed by then are eliminated in a procedure 1301. Next, it acquires based on the node which had the inspection activation means information D ("the inspection activation means information D" is hereafter called "D") related with the node by the screen generation phase of processing in the first half at the time of starting clicked (procedure 1302). Next, detail explanation is taken out from D and it displays on the inspection parameter area 402 (procedure 1303).

[0069] When the node of the inspection activation means of "sendmail_vuln" is chosen as drawing 22 , the example of a screen of the phase where detail explanation was displayed is shown. Next, the actuation which sets up an activation parameter list is explained.

[0070] Next, the activation parameter list Pm of an inspection activation means is acquired from D (procedure 1304), and the procedure parameter P ("the procedure parameter P" is hereafter called "P") is acquired from

the procedure information related with the parent node of the node clicked further (procedure 1305).
[0071] Hereafter, the procedures 1307-1314 as well as procedures 1207-1214 are processed. By processing 1315, it inspects whether the parameter of the parameter name of P [i] and a same name exists in Pm. If it does not exist, since it is the parameter of input needlessness, the item makes the input of displayed GUI improper with this inspection activation means (procedure 1317).
[0072] An example of the screen generated by the above processing is an inspection parameter area in drawing 23 . In drawing 22 and drawing 23 , it is a field [that a "GUI storing directory name" cannot input]. Moreover, an example which generates the inspection parameter area at the time of procedure node selection to drawing 24 is shown. Moreover, an example which generates the inspection parameter area at the time of node selection of an inspection activation means to drawing 25 is shown.
[0073] As shown in drawing, a procedure parameter is a list of executable parameters needed in order to perform all the inspection activation means belonging to inspection routine. A procedure parameter is generated by taking the sum-set of the activation parameter list (an example is shown in drawing 16) contained in the information on an inspection activation means. Moreover, when the node of an inspection activation means is chosen, as shown in drawing 25 , the input only of the activation parameter list contained in the information on the inspection activation means matched with the inspection activation means is enabled, or a default is displayed.
[0074] The processing made into the default of the input parameter of other inspection of an inspection activation result is explained to the last, referring to drawing 26 and drawing 27 . With the gestalt of this operation, an inspection result returns the list which makes (a data name, data type, and a value) one entry as acquired data besides a success and failure. An operating set acquires an inspection result R ("an inspection result R" is hereafter called "R") from inspection activation equipment after performing inspection by 1501 (procedure 1502).
[0075] Next, it checks whether the entry of the parameter which had the identifier of the data name included in R and a same name in the procedure parameter list of the procedure data D related with the next node of the procedure node to which performed inspection belongs exists. If it exists, the data with which it corresponds in R as a default of the parameter will be set up (procedures 1506-1512).
[0076] An inspection activation result can be made into the default of the input parameter of other inspection by applying to all the procedure nodes after the procedure node to which inspection which performed the above-mentioned processing belongs (procedure 1504).
[0077] By the system shown with the gestalt of this operation, a security hole diagnostic tool with the following descriptions is realizable.
[0078] First, the attribute name (sort key name) and procedure execution sequence of inspection activation means information which are used [1st] for a classification are given as a procedure definition, and there is the description that a user without knowledge can also perform inspection of each [sequence adapted to general attack procedure] by classifying the inspection item at the time of activation.
[0079] Furthermore, there is the description of making possible what is visually grasped about whether which inspection having been successful in how far the present inspection being conducted for the user, and changing the display of the node in a procedure viewing area according to each running state of an inspection item having gone wrong.
[0080] Furthermore, there is the description that it can respond to an addition, deletion, and modification of an inspection activation means flexibly by generating dynamically the input screen of each inspection activation means and the parameter needed with inspection routine. By editing the inspection activation means stored in the inspection activation means storing section 504 before inspection activation, an addition and deletion are performed and a change of an inspection activation means is made.
[0081] Furthermore, there is the description that the data with which an inspection activation means outputs the data obtained by the activation result of an inspection activation means by expressing by the list which makes (a data name, data type, and a value) one entry can be set up flexibly.
[0082] Furthermore, there is the description that an input of a user is mitigable by the thing after it automatically set up as a default of the input parameter of inspection, about the data of the inspection result acquired in the form of the above-mentioned description.
[0083] With the gestalt 1 of the gestalt 2. above-mentioned implementation of operation, although three kinds of screens were shown in the operating set, it is not necessarily restricted to this. This security hole diagnostic method may be the case where it has the screen into which a procedure definition file is edited. In this case,

beforehand, fundamental inspection routine is displayed and the screen into which a user edits the displayed inspection routine is offered.
[0084] For example, the screen which performs the following modification is offered.
(1) Change the inspection activation means corresponding to an inspection name (an addition, deletion).
(2) Change the sequence of inspection of inspection routine.
(3) Change the sequence of performing two or more inspection activation means to correspond to an inspection name.
You may be modification other than the above.
[0085] Moreover, it is also possible to offer the screen which changes the default of the executable parameter contained in the information on the inspection activation means corresponding to two or more inspection activation means of each (inspection execution information) or the item of an executable parameter.
[0086]
[Effect of the Invention] According to the security hole diagnostic method concerning this invention, a thing without the detailed knowledge about an inspection activation means can also perform inspection.
[0087] According to the actuation screen of this security hole diagnostic method, the fundamental procedure of inspection routine required for a security hole diagnosis can be grasped.
[0088] According to the actuation screen of this security hole diagnostic method, the inspection activation means corresponding to a procedure can be grasped.
[0089] According to the actuation screen of this security hole diagnostic method, an executable parameter required in order to perform a procedure can be grasped.
[0090] According to the actuation screen of this security hole diagnostic method, the executable parameter for which an input is needed can be known, and a required parameter can be inputted by the actuation control section.
[0091] According to the actuation screen of this security hole diagnostic method, the sequence of performing the inspection activation means corresponding to each inspection name can be grasped.
[0092] According to the actuation screen of this security hole diagnostic method, the procedure parameter (sum-set of an executable parameter) corresponding to an inspection name can be grasped.
[0093] According to the actuation screen of this security hole diagnostic method, an executable parameter required for an inspection activation means can be grasped.
[0094] According to the actuation screen of this security hole diagnostic method, from equipment to be examined, an inspection result can be acquired and the following inspection activation means can be performed using the acquired inspection result.
[0095] According to this security hole diagnostic method, an inspection result can be displayed.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] Drawing showing an example of the whole system of the security hole diagnostic method of the gestalt 1 of operation.
[Drawing 2] Drawing showing an example of the configuration of the inspection activation equipment of the gestalt 1 of operation.
[Drawing 3] Drawing showing an example of the configuration of the operating set of the gestalt 1 of operation.
[Drawing 4] Drawing showing an example of the format of the procedure definition file of the gestalt 1 of operation.
[Drawing 5] Drawing showing an example of the format of the display name definition file of the gestalt 1 of operation.
[Drawing 6] Drawing showing an example of the configuration of the main screen (actuation screen) displayed on that of the operating set of the gestalt 1 of operation.
[Drawing 7] Drawing showing an example of the configuration of the candidate host information input screen displayed on the operating set of the gestalt 1 of operation.
[Drawing 8] Drawing showing an example of the configuration of the inspection result display screen displayed on the operating set of the gestalt 1 of operation.
[Drawing 9] Drawing showing an example of the mark which shows the execution information of the inspection activation means of the main screen displayed on the operating set of the gestalt 1 of operation.
[Drawing 10] The flow Fig. showing an example of actuation of the classification procedure (information reading phase) of an inspection activation means.
[Drawing 11] The flow Fig. showing an example of actuation of the initialization procedure (procedure parameter generation phase) of the inspection routine information at the time of initialization.
[Drawing 12] The flow Fig. showing an example of actuation of the initial-screen construction procedure (screen-display phase) in the procedure viewing area 401.
[Drawing 13] Drawing explaining the contents of the procedure definition file.
[Drawing 14] Drawing explaining the information on an inspection activation means.
[Drawing 15] Drawing explaining the case where information on an inspection activation means is ****(ed) by property name "PLUGIN_TYPE".
[Drawing 16] Drawing explaining the activation parameter list of the information on an inspection activation means.
[Drawing 17] Drawing showing an example of actuation of procedure parameter area generation when a user chooses a procedure node by the procedure viewing area of the main screen.
[Drawing 18] Drawing showing an example of actuation of procedure parameter area generation when a user chooses a procedure node by the procedure viewing area of the main screen.
[Drawing 19] Drawing showing an example of the procedure parameter area generated when a user chose a procedure node by the procedure viewing area of the main screen.
[Drawing 20] Drawing showing an example of actuation of procedure parameter area generation when a user chooses the node of an inspection activation means by the procedure viewing area of the main screen.
[Drawing 21] Drawing showing an example of actuation of procedure parameter area generation when a user chooses the node of an inspection activation means by the procedure viewing area of the main screen.
[Drawing 22] Drawing showing an example of the procedure parameter area (before an executable parameter setup) generated when a user chose the node of an inspection activation means by the procedure viewing area

of the main screen.
[Drawing 23] Drawing showing an example of the procedure parameter area (after an executable parameter setup) generated when a user chose the node of an inspection activation means by the procedure viewing area of the main screen.
[Drawing 24] Drawing explaining the procedure parameter of an inspection parameter area when a user chooses a procedure node by the procedure viewing area of the main screen.
[Drawing 25] Drawing explaining the executable parameter of an inspection parameter area when a user chooses the node of an inspection activation means by the procedure viewing area of the main screen.
[Drawing 26] Drawing showing an example of the actuation for reusing the inspection result of the inspection activation means of 1 to the next inspection.
[Drawing 27] Drawing showing an example of the actuation for reusing the inspection result of the inspection activation means of 1 to the next inspection.
[Description of Notations]
103 Network, 104 Host to Be Examined, 200 Operating Set, The 201 screen generation section, 202 A procedure definition file, 203 Display name definition file, 204 An actuation control section, 205 A display, 301 Main screen (actuation screen), The host information input screen for 302, 303 The inspection result display screen, 401 Procedure viewing area, 402 An inspection parameter area, 500 Inspection activation equipment, 501 The execution control section, 502 The candidate host information storing section, 503 An inspection activation means, 504 The inspection activation means storing section, 901-904 Mark showing the activation situation of inspection.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－337919
（P2001－337919A）
(43)公開日　平成13年12月７日(2001.12.7)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ａ	５Ｂ０４８
	11/22	３１０	11/22	３１０Ｒ	５Ｂ０８５

審査請求　未請求　請求項の数10　ＯＬ　（全 21 頁）

(21)出願番号　特願2000－153601(P2000－153601)

(22)出願日　平成12年５月24日(2000.5.24)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

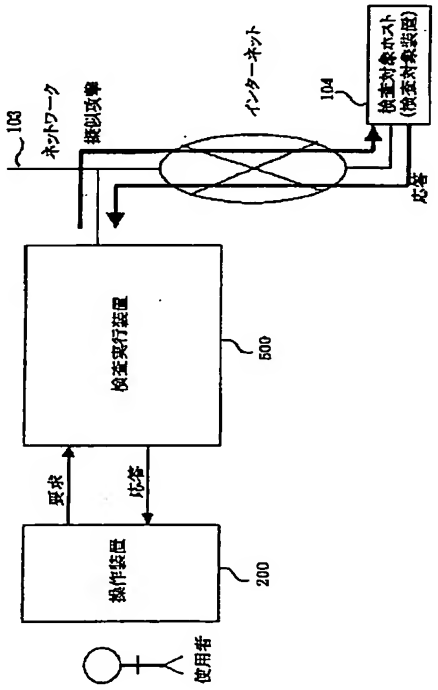
(72)発明者　河内　清人
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　100099461
弁理士　溝井　章司　（外２名）

Ｆターム(参考)　5B048 AA18 CC15 DD08 EE00
5B085 AC08 CE01

(54)【発明の名称】　セキュリティホール診断方式

(57)【要約】
【課題】　検査を容易に実行できるような検査手順を提供する。
【解決手段】　セキュリティホール診断方式は、検査実行装置５００と操作装置２００とを備え、検査実行装置５００は、検査対象ホスト１０４を検査する複数の検査実行手段５０３と、複数の検査実行手段５０３の情報を定義する複数の検査実行情報とを格納する検査実行手段格納部５０４と、複数の検査実行手段の実行と操作装置２００とのインタフェースとを制御する実行制御部５０１とを備え、操作装置２００は、検査実行装置５００とのインタフェースを制御し、利用者から入力される指示を受け付ける操作制御部２０４と、検査実行手段５０３を用いてセキュリティホールを診断する検査を示す検査名を、検査する順序に従って定義する検査手順を記憶する手順定義ファイル２０２と、検査名と検査実行手段名とを表示する操作画面を上記ディスプレイに表示する画面生成部２０１とを備える。



1

【特許請求の範囲】

【請求項１】　ディスプレイ有し、ディスプレイに表示される画面に基づいて利用者から入力される指示を受け付ける操作装置と、セキュリティホールを診断する検査対象装置へ検査を実行する検査実行装置とを備えたセキュリティホール診断方式において、

上記検査実行装置は、

検査対象装置を検査する複数の検査実行手段と、

上記複数の検査実行手段それぞれを示す検査実行手段名を含む情報を上記複数の検査実行手段それぞれに対応させて定義する複数の検査実行情報と、上記複数の検査実行手段とを対応づけて格納する検査実行手段格納部と、

上記複数の検査実行手段の実行を制御し、上記操作装置とのインタフェースとを制御する実行制御部とを備え、

上記操作装置は、

上記検査実行装置とのインタフェースを制御し、利用者から入力される指示を受け付ける操作制御部と、

上記検査実行手段を用いてセキュリティホールを診断する検査を示す検査名を、検査する順序に従って定義する検査手順を記憶する手順定義ファイルと、

上記手順定義ファイルから検査手順を読み込み、読み込んだ検査手順に基づいて、上記操作制御部を介して上記検査実行手段格納部から検査実行情報を取得し、上記検査手順と取得した検査実行情報とに基づいて、検査名と検査実行手段名とを表示する操作画面を生成し、生成した操作画面を上記ディスプレイに表示する画面生成部とを備えることを特徴とするセキュリティホール診断方式。

【請求項２】　上記手順定義ファイルは、検査手順として、複数の検査名と、上記複数の検査名それぞれに対応する詳細情報とを記憶し、

上記画面生成部は、上記手順定義ファイルから検査手順を読み込み、読み込んだ検査手順に含まれる複数の検査名を表示する操作画面を生成し、

上記操作制御部は、操作画面に表示された複数の検査名のうち、利用者によって選択される検査名の入力を受け付け、受け付けた検査名を上記画面生成部に通知し、

上記画面生成部は、上記操作制御部から通知された上記検査名を入力し、入力した検査名に対応する詳細情報を上記検査手順ファイルから読み込み、読み込んだ詳細情報を表示する操作画面を生成することを特徴とする請求項１記載のセキュリティホール診断方式。

【請求項３】　上記検査実行情報は、検査名を含み、

上記画面生成部は、取得した検査実行情報に含まれる検査名を抽出し、抽出した検査名と対応する検査実行手段名とを対応させて操作画面を生成することを特徴とする請求項１または２記載のセキュリティホール診断方式。

【請求項４】　上記検査実行情報は、検査実行手段の実行に必要な実行パラメータを含み、

上記操作画面は、上記検査名と検査実行手段名と対応づけて表示する手順表示領域と、上記実行パラメータを表示する検査パラメータ領域とを含み、

2

上記操作制御部は、利用者によって選択される検査実行手段名の入力を受け付け、受け付けた検査実行手段名を上記画面生成部へ通知し、

上記画面生成部は、上記操作制御部から通知された検査実行手段名を入力し、上記操作制御部を介して上記検査実行装置の検査実行手段格納部から、入力した検査実行手段名が示す検査実行手段に対応する検査実行情報を取得し、取得した検査実行情報から実行パラメータを抽出し、抽出した実行パラメータを検査パラメータ領域に表示する操作画面を生成することを特徴とする請求項１から３いずれかに記載のセキュリティホール診断方式。

【請求項５】　上記検査パラメータ領域は、実行パラメータの入力を受け付ける入力領域を含み、

上記操作制御部は、利用者によって入力された実行パラメータを受け付け、受け付けた実行パラメータを上記実行制御部へ出力し、

上記実行制御部は、上記操作制御部から実行パラメータを入力し、入力した実行パラメータを用いて、検査実行手段を実行させることを特徴とする請求項４記載のセキュリティホール診断方式。

【請求項６】　上記セキュリティホールを診断する検査は、複数の検査実行手段を用いて実行され、

上記検査名は、複数の検査実行手段名と対応づけられ、

上記検査実行情報は、検査に用いられる複数の検査実行手段のうち何番目に実行するかを示す実行番号を含み、

上記画面生成部は、上記検査名に対応づけられる複数の検査実行手段名それぞれを含む複数の検査実行情報を取得し、取得した複数の検査実行情報それぞれから複数の検査実行手段名と複数の実行番号とを抽出し、抽出した複数の実行番号それぞれに基づいて、上記検査名と抽出した複数の検査実行手段名とを手順表示領域に表示する操作画面を生成することを特徴とする請求項５記載のセキュリティホール診断方式。

【請求項７】　上記画面生成部は、取得した複数の検査実行情報それぞれから実行パラメータを抽出し、抽出した実行パラメータの内、実行する検査名に対応する複数の検査実行情報それぞれに含まれる実行パラメータを手順パラメータとして生成し、生成した手順パラメータを上記手順パラメータ領域に表示する操作画面を生成することを特徴とする請求項６記載のセキュリティホール診断方式。

【請求項８】　上記操作制御部は、上記複数の検査実行手段名のうち、利用者によって選択された検査実行手段名の入力を受け付け、受け付けた検査実行手段名を上記画面生成部に出力し、

上記画面生成部は、上記操作制御部から上記検査実行手段名を入力し、入力した検査実行手段名に対応する実行パラメータを検査パラメータ領域に表示する操作画面を

生成することを特徴とする請求項６記載のセキュリティホール診断方式。

【請求項９】　上記実行制御部は、検査対象装置から検査実行結果を取得し、取得した検査実行結果を検査実行情報へ書き込み、上記実行制御部を介して検査実行結果を書き込んだ検査実行情報を上記操作制御部へ出力し、

上記操作制御部は、上記実行制御部から出力された検査実行情報を入力し、入力した検査実行情報に含まれる検査実行結果を上記画面生成部へ通知し、

上記画面生成部は、通知された検査実行結果を入力し、入力した検査実行結果を上記実行パラメータとして検査パラメータ領域に表示する操作画面を生成することを特徴とする請求項６記載のセキュリティホール診断方式。

【請求項１０】　上記実行制御部は、検査実行手段を用いてセキュリティホールの診断する検査の実行状況を検査対象装置から取得し、取得した検査の実行状況を操作制御部へ出力し、

上記操作制御部は、上記実行制御部から出力された検査の実行状況を入力し、入力した検査の実行状況を上記画面生成部へ通知し、

上記画面生成部は、上記操作制御部から通知された検査の実行状況を取得し、取得した検査の実行状況を表示する検査結果表示画面を生成し、生成した検査結果表示画面を上記ディスプレイに表示することを特徴とする請求項１記載のセキュリティホール診断方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータのセキュリティホールの有無を診断するシステムに関するものである。

【０００２】

【従来の技術】従来、網羅的なセキュリティホールの診断ツールとして、例えば、Ｉｎｔｅｒｎｅｔ　Ｓｅｃｕｒｉｔｙ　Ｓｙｓｔｅｍｓ社のＩｎｔｅｒｎｅｔ　Ｓｃａｎｎｅｒや、フリーで公開されているｎｅｓｓｕｓが挙げられる。これらは、既知のセキュリティホールのデータベースを持ち、外部から検査対象ホストに対してセキュリティホールの有無を検査する機能を有する。

【０００３】一方、実際に攻撃を行うことでセキュリティホールの検査を行うツールとして、ｎｍａｐや、Ｊｏｈｎ　ｔｈｅ　ｒｉｐｐｅｒと呼ばれるツールが存在する。ｎｍａｐは対象ホスト上で稼動しているサービスを特定するためのツールであり、Ｊｏｈｎ　ｔｈｅ　ｒｉｐｐｅｒはパスワードファイルを入力として脆弱なパスワードを持ったアカウントを検出するツールである。

【０００４】

【発明が解決しようとする課題】しかし、上記のような網羅的なセキュリティホール診断ツールは、検査対象ホストのセキュリティホールの存在を確認するのみであり、そのセキュリティホールを使ってさらに、どのような不正アクセスが可能かまでは判定を行わない。そのため、管理者が上記ツールを使って管理下に置かれているコンピュータ上にセキュリティホールを発見したとしても、過去にどの程度まで侵入された可能性があるかは、管理者の知識と経験に頼らなければならないという問題点があった。

【０００５】上述したように、どの程度まで侵入される可能性があるかの検査は、実際に攻撃を行ってみる必要があるが、既存の攻撃ツールは、単機能を実現したものばかりであり、それらをどのような手順で用いれば効果的な攻撃になるのか、また、あるツールで得られた情報を他のツールでどのように応用すれば良いのかは、使用者の技量に依存する部分が大きかった。

【０００６】本発明は、上記の問題点を解消するためになされたものであり、単機能の検査を複数用意し、それらを一般に効果的と思われる検査手順に従って分類し、各検査結果を他の検査に自動的に再利用することを可能とした統合的セキュリティホール診断ツールである。

【０００７】

【課題を解決するための手段】この発明に係るセキュリティホール診断方式は、ディスプレイ有し、ディスプレイに表示される画面に基づいて利用者から入力される指示を受け付ける操作装置と、セキュリティホールを診断する検査対象装置へ検査を実行する検査実行装置とを備えたセキュリティホール診断方式において、上記検査実行装置は、検査対象装置を検査する複数の検査実行手段と、上記複数の検査実行手段それぞれを示す検査実行手段名を含む情報を上記複数の検査実行手段それぞれに対応させて定義する複数の検査実行情報と、上記複数の検査実行手段とを対応づけて格納する検査実行手段格納部と、上記複数の検査実行手段の実行を制御し、上記操作装置とのインタフェースとを制御する実行制御部とを備え、上記操作装置は、上記検査実行装置とのインタフェースを制御し、利用者から入力される指示を受け付ける操作制御部と、上記検査実行手段を用いてセキュリティホールを診断する検査を示す検査名を、検査する順序に従って定義する検査手順を記憶する手順定義ファイルと、上記手順定義ファイルから検査手順を読み込み、読み込んだ検査手順に基づいて、上記操作制御部を介して上記検査実行手段格納部から検査実行情報を取得し、上記検査手順と取得した検査実行情報とに基づいて、検査名と検査実行手段名とを表示する操作画面を生成し、生成した操作画面を上記ディスプレイに表示する画面生成部とを備えることを特徴とする。

【０００８】上記手順定義ファイルは、検査手順として、複数の検査名と、上記複数の検査名それぞれに対応する詳細情報とを記憶し、上記画面生成部は、上記手順定義ファイルから検査手順を読み込み、読み込んだ検査手順に含まれる複数の検査名を表示する操作画面を生成し、上記操作制御部は、操作画面に表示された複数の検

査名のうち、利用者によって選択される検査名の入力を受け付け、受け付けた検査名を上記画面生成部に通知し、上記画面生成部は、上記操作制御部から通知された上記検査名を入力し、入力した検査名に対応する詳細情報を上記検査手順ファイルから読み込み、読み込んだ詳細情報を表示する操作画面を生成することを特徴とする。

【０００９】上記検査実行情報は、検査名を含み、上記画面生成部は、取得した検査実行情報に含まれる検査名を抽出し、抽出した検査名と対応する検査実行手段名とを対応させて操作画面を生成することを特徴とする。

【００１０】上記検査実行情報は、検査実行手段の実行に必要な実行パラメータを含み、上記操作画面は、上記検査名と検査実行手段名と対応づけて表示する手順表示領域と、上記実行パラメータを表示する検査パラメータ領域とを含み、上記操作制御部は、利用者によって選択される検査実行手段名の入力を受け付け、受け付けた検査実行手段名を上記画面生成部へ通知し、上記画面生成部は、上記操作制御部から通知された検査実行手段名を入力し、上記操作制御部を介して上記検査実行装置の検査実行手段格納部から、入力した検査実行手段名が示す検査実行手段に対応する検査実行情報を取得し、取得した検査実行情報から実行パラメータを抽出し、抽出した実行パラメータを検査パラメータ領域に表示する操作画面を生成することを特徴とする。

【００１１】上記検査パラメータ領域は、実行パラメータの入力を受け付ける入力領域を含み、上記操作制御部は、利用者によって入力された実行パラメータを受け付け、受け付けた実行パラメータを上記実行制御部へ出力し、上記実行制御部は、上記操作制御部から実行パラメータを入力し、入力した実行パラメータを用いて、検査実行手段を実行させることを特徴とする。

【００１２】上記セキュリティホールを診断する検査は、複数の検査実行手段を用いて実行され、上記検査名は、複数の検査実行手段名と対応づけられ、上記検査実行情報は、検査に用いられる複数の検査実行手段のうち何番目に実行するかを示す実行番号を含み、上記画面生成部は、上記検査名に対応づけられる複数の検査実行手段名それぞれを含む複数の検査実行情報を取得し、取得した複数の検査実行情報それぞれから複数の検査実行手段名と複数の実行番号とを抽出し、抽出した複数の実行番号それぞれに基づいて、上記検査名と抽出した複数の検査実行手段名とを手順表示領域に表示する操作画面を生成することを特徴とする。

【００１３】上記画面生成部は、取得した複数の検査実行情報それぞれから実行パラメータを抽出し、抽出した実行パラメータの内、実行する検査名に対応する複数の検査実行情報それぞれに含まれる実行パラメータを手順パラメータとして生成し、生成した手順パラメータを上記手順パラメータ領域に表示する操作画面を生成することを特徴とする。

【００１４】上記操作制御部は、上記複数の検査実行手段名のうち、利用者によって選択された検査実行手段名の入力を受け付け、受け付けた検査実行手段名を上記画面生成部に出力し、上記画面生成部は、上記操作制御部から上記検査実行手段名を入力し、入力した検査実行手段名に対応する実行パラメータを検査パラメータ領域に表示する操作画面を生成することを特徴とする。

【００１５】上記実行制御部は、検査対象装置から検査実行結果を取得し、取得した検査実行結果を検査実行情報へ書き込み、上記実行制御部を介して検査実行結果を書き込んだ検査実行情報を上記操作制御部へ出力し、上記操作制御部は、上記実行制御部から出力された検査実行情報を入力し、入力した検査実行情報に含まれる検査実行結果を上記画面生成部へ通知し、上記画面生成部は、通知された検査実行結果を入力し、入力した検査実行結果を上記実行パラメータとして検査パラメータ領域に表示する操作画面を生成することを特徴とする。

【００１６】上記実行制御部は、検査実行手段を用いてセキュリティホールの診断する検査の実行状況を検査対象装置から取得し、取得した検査の実行状況を操作制御部へ出力し、上記操作制御部は、上記実行制御部から出力された検査の実行状況を入力し、入力した検査の実行状況を上記画面生成部へ通知し、上記画面生成部は、上記操作制御部から通知された検査の実行状況を取得し、取得した検査の実行状況を表示する検査結果表示画面を生成し、生成した検査結果表示画面を上記ディスプレイに表示することを特徴とする。

【００１７】

【発明の実施の形態】実施の形態１．以下、図を参照しながら本実施の形態の動作を述べる。はじめに、図１を参照しながらシステム全体の動作について説明する。本システムは、検査対象ホスト１０４に対してネットワーク１０３を通じて擬似攻撃を行うことで、検査対象ホスト（検査対象装置）１０４に存在するセキュリティホールを検出するものである。

【００１８】本システムは、操作装置２００、検査実行装置５００で構成されており、使用者は操作装置２００を通じて検査実行装置５００に検査要求を送り、検査実行装置５００から返される検査の実行結果が操作装置２００上に表示される。

【００１９】次に、図２を参照しながら検査実行装置５００の構成の一例について説明する。検査実行装置５００は、実行制御部５０１、対象ホスト情報格納部５０２、検査実行手段５０３、検査実行手段格納部５０４で構成されている。

【００２０】実行制御部５０１は、操作装置２００からの要求に応じて検査実行装置５００全体を制御する。各擬似攻撃は、検査実行手段５０３上に実装されている。検査実行手段５０３は、検査実行手段格納部５０４中に

格納されている。検査実行手段５０３は、必要に応じて実行制御部５０１によってメモリ上にロードされ、擬似攻撃を実行する。

【００２１】対象ホスト情報格納部５０２は、操作装置２００から、もしくは擬似攻撃から得られた検査対象ホスト１０４に関する情報を蓄え、別の擬似攻撃を行う際の情報として利用できるようにするためのものである。一例を挙げれば、操作装置２００から検査対象ホストのＩＰアドレスが格納されたり、ポートスキャン擬似攻撃によって取得された対象ホスト上のポート情報が格納されたりする。それらは、別の検査実行手段によって参照される。

【００２２】また、検査実行手段格納部５０４は、複数の検査実行手段５０３を格納するとともに、併せて、検査実行手段に対応する情報を検査実行手段の情報（検査実行情報）として格納する。検査実行手段の情報は、検査実行手段５０３の内部に記録されている場合もある。

【００２３】検査実行手段の情報は、検査実行手段５０３と対応づけられて上記検査実行手段格納部に格納されていればよい。従って、検査実行手段５０３の内部に記録されている場合でも、別個のファイルとして存在する場合でもよい。以下の説明では、検査実行手段５０３の内部に、検査実行手段の情報が記録されている場合を説明する。

【００２４】次に、図３を参照しながら操作装置２００について説明する。操作装置２００は、画面生成部２０１と、手順定義ファイル２０２と、表示名定義ファイル２０３と、操作制御部２０４と、ディスプレイ２０５とを備える。操作制御部２０４は、検査実行装置とのインタフェースを制御し、利用者から入力される指示を受け付ける。この他、操作制御部２０４は、操作装置２００全体を制御する。手順定義ファイル２０２は、セキュリティホール診断の検査手順を検査する順序に従って定義する。

【００２５】画面生成部２０１は、手順定義ファイル２０２から検査手順を読み込み、読み込んだ検査手順に基づいて、操作制御部２０４を介して検査実行手段格納部５０４から検査手順手段の情報検査実行情報（検査実行情報）を取得し、取得した検査実行手段の情報と、検査手順に基づいて、検査手順を表示する操作画面を生成し、生成した操作画面を上記ディスプレイ２０５に表示する。

【００２６】操作装置２００は、操作画面によって使用者に操作手段を提供する。操作画面制御部２０４は、起動時に手順定義ファイル２０２、表示名定義ファイル２０３を読み込み必要な初期化を行う。

【００２７】手順定義ファイル２０２は、手順名、手順の補足情報（実行条件、詳細説明）及び各手順に検査実行手段を分類するためのルールを記述したものであり、「ポートスキャン」、「ファイル取得」といった一般的な攻撃手順を検査手順（以下、「検査手順」を「手順」ともいう）として定義したものである。操作装置起動時に、各検査手順に属する検査実行手段が検索・ソートされ、画面に表示される。図４は、この実施の形態の手順定義ファイル２０２の書式の一例を示している。

【００２８】表示名定義ファイル２０３は、画面上に表示される文字列を各国語に変換するための辞書である。図５は、この実施の形態の表示名定義ファイル２０３の書式の一例を示している。

【００２９】図６から図８に操作画面の一例を示している。図６は、主画面（操作画面）３０１の一例を示している。主画面３０１は、検査手順を表示する手順表示領域４０１と、検査実行手段５０３で使用する検査パラメータ領域４０２とを備える。図７は、対象ホスト情報入力画面３０２の一例を示している。図８は、検査結果表示画面３０３の一例を示している。

【００３０】手順表示領域４０１は、本システムで実行可能な「検査手順」をツリーのノードとして表示し、さらに各「検査手順」に対応する検査実行手段名をそのサブノードとして表示する。

【００３１】検査パラメータ領域４０２は、手順表示領域４０１上で選択された「検査手順」もしくは検査実行手段名に対応して生成され、選択した手順、もしくは検査を実行するために必要なパラメータを入力するための画面を表示する。

【００３２】これらの操作画面は、必要に応じて表示・消去される。対象ホスト情報入力画面３０２は、検査実行装置５００中の対象ホスト情報格納部５０２中に格納されている情報の表示・編集を行うための画面である。利用者は、対象ホスト情報入力画面３０２を用いて検査する装置を指定する。検査結果表示画面３０３は、検査の実行結果を表示する画面である。

【００３３】本操作装置２００の操作方法について簡単に述べる。使用者が操作装置２００を起動すると、図６に示される主画面３０１が表示される。手順表示領域４０１には、検査手順を表す検査手順のノード（手順ノード）が表示される。また、そのサブノードとして、各手順に分類された検査実行手段名（検査実行手段のノード）が表示されている。

【００３４】使用者が、検査手順のノード（手順ノード）、もしくは検査実行手段のノードを選択すると、対応したパラメータ入力画面が検査パラメータ領域４０２上に生成される。これは、選択したノードに対応する検査を実行するために、使用者が与えなければならない実行時パラメータの入力項目を表すものである。手順ノードを選択した場合、その検査手順に分類される全ての検査実行手段５０３を実行するために必要なパラメータが全て表示される。

【００３５】検査実行手段のノードを選択した状態で検査を行った場合にはそれだけを実行する。手順ノードを

選択した状態で検査を行った場合には、選択した手順ノードにサブノードとして所属する検査実行手段を順に実行していく。実行結果は、検査結果表示画面３０３で確認することができる。

【００３６】手順ノードを選択して検査を行った場合、その検査手順の性質上、「どれか一つでも成功すれば良い」ものと、「全てを実行したほうが良い」ものが考えられる。例えば、「ファイル取得」の手順は、内包する検査実行手段のどれか一つでも成功すれば目的は達成できるが、「ポートスキャン」の場合は、内包する検査実行手段を全て実行した場合に、成果を最大化することができる。

【００３７】これらを使用者が制御できるようにするために、本実施の形態では、手順ノードを選択した場合に、検査パラメータ領域４０２上に、実行終了条件選択用ラジオボタンを表示するようにしている。ラジオボタンは、「成功した時点で終了」、「全て実行」、「ユーザに問い合わせ」の３種類から選択することができる。利用者は、上記３種類から１つを選択する。

【００３８】図９は、操作画面における検査実行手段の実行状態の表示方法を示す図である。検査の実行状況は、図９で表されるアイコンを対応する手順表示領域４０１中のノードに表示することで使用者に通知される。

【００３９】検査の結果、「パスワードファイル」を取得できたり、アカウントやパスワードが明らかになる場合がある。次に、入力パラメータとしてそれらを必要とする検査手順、もしくは検査実行手段を選択したとき、それら取得されたデータがデフォルト値として検査パラメータ領域４０２中のパラメータ入力用ＧＵＩにセットされる。

【００４０】次に、本システムの動作について説明する。はじめに、図１０，図１１及び図１２を参照しながら、起動時の処理について説明する。起動時の処理は大きく３つに分類される。情報読み込み段階、手順パラメータ生成段階、画面表示段階である。

【００４１】図１０は、操作画面における検査実行手段の分類手順（情報読み込み段階）を示すフローチャートである。図１１は、初期化時における検査手順情報の初期化手順（手順パラメータ生成段階）を示すフローチャートである。図１２は、操作画面における手順表示領域４０１における初期画面構築手順（画面表示段階）を示すフローチャートである。以下、順を追って説明する。

【００４２】図１０は、情報読み込み段階を表すフローチャートである。システム起動時、８０１でシステムは、手順定義ファイル２０２を読み込む。手順定義ファイルは、図４で示されるような形式をしており、分類キー名と、手順定義エントリ（キー値、カテゴリ名（手順表示名）、実行終了条件、詳細説明）のリストで構成されている。

【００４３】図４では、分類キー名は、ＰＬＵＧＩＮ＿ＴＹＰＥを一例として示している。また、図４では、手順定義エントリは、〈キー値〉＝〈カテゴリ名（手順表示名）〉￥〈実行終了条件〉￥〈詳細説明〉の書式で記述されている。

【００４４】図１３に、手順定義ファイルの構成の一例を示している。手順定義ファイルには、上述の様に、分類キー名と、「キー値＝分類先カテゴリ情報」として表わされている手順定義エントリを含む。分類先カテゴリ情報は、カテゴリ名（手順表示名）と実行終了条件と詳細説明の部分が相当する。

【００４５】図１３に、カテゴリ名、実行終了条件、詳細説明の使用方法を示している。

【００４６】次に、８０２で、読み込まれた手順定義エントリのリストから、キー値で検索可能な手順データ辞書（Ｍａｐ）を生成する。Ｍａｐに格納されるデータは、（手順表示名（カテゴリ名）、実行終了条件、手順説明（手順定義エントリの詳細説明）、検査実行手段情報のリスト、手順パラメータ）の要素を持った構造体である。検査実行手段情報のリスト及び手順パラメータは、この段階では空である。

【００４７】８０３～８０９で、検査実行装置５００の検査実行手段格納部５０４中に格納されている全ての検査実行手段５０３から検査実行手段の情報を取得する。取得した検査実行手段の情報は、分類キー名をプロパティ名として検索し、検索した結果として、キー値を取得する。取得したキー値でＭａｐを検索し、該当する手順データ中の検査実行手段情報のリストに登録していく。

【００４８】まず、画面生成部２０１は、手順定義ファイルを読み込み、分類キー名を取得（例えば、図４の手順定義ファイルでは、“ＰＬＵＧＩＮ＿ＴＹＰＥ”）する。次に、画面生成部２０１は、操作制御部２０４を介して、検査実行装置５００の検査実行手段格納部５０４に格納されている検査実行手段５０３を読み出し、検査実行手段の情報を取得する。図１４に、検査実行手段５０３と検査実行手段の情報との関係を示している。

【００４９】次に、画面生成部２０１は、取得した検査実行手段の情報から分類キー名（ここでは、“ＰＬＵＧＩＮ＿ＴＹＰＥ”）に該当するデータの値を取得する。図１５に、データの値を取得する様子を示している。ここで、取得したデータの値が手順定義ファイル２０２中のキー値に対応している。

【００５０】取り出された値（ここでは、“ＰＡＳＳＷＯＲＤ＿ＣＲＡＣＫ”）を元に、手順定義ファイル２０２内で該当する分類先カテゴリを検索する。該当する分類先カテゴリに対応する画面上のノードの子ノードとして、検査実行手段ノードを生成する。生成するノードの名前は、検査実行手段の情報の実行検査名（“ＮＡＭＥ”）プロパティ（図１５の場合は、“ｊｏｈｎ”）を使用する。

【００５１】２～５の過程を保存されている全ての検査

実行手段について行う。

【００５２】検査実行手段の情報は、図１５に示すように、プロパティ名、データ型、値を１エントリとするデータのリストである。このリストが複数存在する。値には、更にリストをネストさせることが可能である。検査実行手段の情報は、少なくとも実行検査名（プロパティ名は、“ＮＡＭＥ”）（文字列型）、実行パラメータリスト（プロパティ名は、“ＰＡＲＡＭＥＴＥＲ”）（リスト型）の２つのプロパティを含む。

【００５３】検査実行手段の情報に含まれるその他の属性は、検査実行手段毎に任意に追加可能である。各属性は、プロパティ名で識別される。検査実行手段の情報は、１のキー値に対応する複数の検査実行手段のうち、何番目に実行する検査実行手段であるかを示す実行番号を含む。

【００５４】図１６は、検査実行手段の情報に含まれる実行パラメータリストの一例を示している。検査実行手段の情報の実行パラメータリストに該当する部分は、プロパティ名を”ＰＡＲＡＭＥＴＥＲ”とする。実行パラメータリストは、パラメータ名、データ型、デフォルト値を１エントリとするデータのリストである。

【００５５】実行パラメータは、検査実行手段を実行する時に検査実行手段に与えなければならないパラメータを規定する。デフォルト値は、パラメータがしてされたかった場合に使用される値である。また、検査実行時に、パラメータの値が許容範囲以外があったり、パラメータが不足ている場合など、パラメータのエラーが発生する場合は、利用者にエラーを警告するメッセージを表示し、パラメータの入力を促す。上記検査実行手段の情報中の実行パラメータリストは、パラメータ名、データ型、デフォルト値を１エントリとするデータのリストである。

【００５６】次に、図１１を参照しながら手順パラメータ生成段階の処理について説明する。この段階の目的は、各「検査手順」に属する検査実行手段情報中に含まれる実行パラメータリスト全てを内包するようなパラメータリストを生成し、それを手順データ中の手順パラメータとして登録することである。

【００５７】図１１で表されるフローチャートは２つのネストしたループで構成されている。一つは１００２～１０１１で表されるループであり、これはＭａｐ内の全ての手順データに渡って１００３～１００９が実行されることを表している。もう一つは１００６～１００９で表されるループであり、これは各手順データ中の検査実行手段情報リストに登録されている全ての検査実行手段情報に渡って１００７～１００８が実行されることを表している。

【００５８】１００７で取得された実行パラメータリストは、全て１００８で合成され、最終結果が１０１０で、手順データ中の手順パラメータとして登録される。１００８で実施される合成とは、中間結果Ｐｔと１００７で取得された実行パラメータリスト（ｐａｒａｍ＿ｌｉｓｔ）とを比較し、Ｐｔ中に存在しないパラメータ名を持ったエントリがｐａｒａｍ＿ｌｉｓｔ中に存在した場合に、そのエントリをＰｔに追加することで実現される。

【００５９】上記処理によって生成される手順パラメータは、その「検査手順」に含まれる全ての検査実行手段を実行するのに最低限必要なパラメータリストを表している。

【００６０】次に、図１２を参照しながら画面表示段階の処理について説明する。図１２で表されるフローチャートは２つのネストしたループで構成されている。外側のループは、１１０２～１１１１で表されるループである。これはＭａｐ内の全ての手順データに渡って、手順表示領域４０１上にノードを生成し、更に、その内部でループ１１０６～１１１０を実行することで、各手順データに登録されている検査実行手段に対応するノードを、手順ノードのサブノードとして生成する。生成された各ノードには、手順データ、もしくは検査実行手段の情報が関連付けられる。以上が、本システム起動時の処理に関する説明である。

【００６１】次に、使用者が手順表示領域４０１上のノードをクリックした時の検査パラメータ領域４０２の生成処理について説明する。図１７，図１８は、使用者が手順表示領域４０１上の検査手順を表すノード（手順ノード）をクリックした場合の検査パラメータ領域４０２の生成処理を表すフローチャートである。手順１２０１で、それまでに表示されていた内容を全て消去する。次に、前期起動時処理の画面生成段階でノードに関連付けられた手順データＤ（以下、「手順データＤ」を「Ｄ」という）をクリックされたノードを元に取得する（手順１２０２）。次に、Ｄから詳細説明を取り出し、検査パラメータ領域４０２上に表示する（手順１２０３）。

【００６２】次に、画面上に実行終了条件を表すラジオボタンを生成し、Ｄに登録されている実行終了条件に対応するラジオボタンを選択状態にする（手順１２０４）。本実施の形態では実行終了条件として、「一つでも成功したら終了」、「全て実行」、「成功したらユーザに問い合わせ」の３通りを用意している。

【００６３】次に、Ｄから手順パラメータリストＰ（以下、「手順パラメータリストＰ」を「Ｐ」という）を取得（手順１２０５）し、Ｐ中の各パラメータエントリに対し、ループ１２０７～１２１５で対応する入力画面を検査パラメータ領域４０２上に表示する。

【００６４】ループ１２０７～１２１５では、次のように処理を行う。Ｐのｉ番目の要素をＰ［ｉ］と表現することにする。まず、手順１２０８でＰ［ｉ］よりパラメータ名を取得し、検査パラメータ領域４０２上に表示する。この時、表示名は起動時に読み込まれた表示名定義

ファイル２０３の内容に従って、判りやすい言葉に変換される。次に、手順１２０９でＰ［ｉ］のデータ型が評価され、その結果によって処理が分岐する。

【００６５】もし、データ型が文字列、もしくは数値であった場合には、先ほど表示したパラメータ名の下に、テキストボックスを表示する（手順１２１０）。テキストボックスには、Ｐ［ｉ］に設定されたデフォルト値が表示される（手順１２１１）。

【００６６】もし、データ型がバイナリであった場合には、パラメータ名の下に、バイナリデータの格納されたファイルのパス名を入力するテキストボックスを表示する（手順１２１２）。次に、パラメータ名の横にバイナリデータが格納されているファイルを選択するためのダイアログを表示する「参照」ボタンを生成する（手順１２１３）。最後に、デフォルト値をＰ［ｉ］から取り出し、テキストボックスにセットする（手順１２１４）。

【００６７】以上の処理によって生成される画面の一例が、図１９中の検査パラメータ領域４０２である。図１９は、表示されているデータの出所も示している。

【００６８】図２０，図２１は、使用者が手順表示領域４０１上の検査実行手段を表すノード（検査実行手段のノード）をクリックした場合の検査パラメータ領域４０２の生成処理を表すフローチャートである。手順１３０１で、それまでに表示されていた内容を全て消去する。次に、前期起動時処理の画面生成段階でノードに関連付けられた検査実行手段情報Ｄ（以下、「検査実行手段情報Ｄ」を「Ｄ」という）をクリックされたノードを元に取得する（手順１３０２）。次に、Ｄから詳細説明を取り出し、検査パラメータ領域４０２上に表示する（手順１３０３）。

【００６９】図２２に、“ｓｅｎｄｍａｉｌ＿ｖｕｌｎ”の検査実行手段のノードを選択したときに、詳細説明が表示された段階の画面例を示している。次に、実行パラメータリストを設定する動作を説明する。

【００７０】次に、Ｄから検査実行手段の実行パラメータリストＰｍを取得し（手順１３０４）、更にクリックされたノードの親ノードに関連付けられた手順情報から手順パラメータＰ（以下、「手順パラメータＰ」を「Ｐ」という）を取得する（手順１３０５）。

【００７１】以下、手順１２０７～１２１４と同様に、手順１３０７～１３１４は処理される。処理１３１５で、Ｐ［ｉ］のパラメータ名と同名のパラメータがＰｍに存在するかどうかを検査する。もし、存在していなければ、その項目は、該検査実行手段では入力不要のパラメータであるので、表示したＧＵＩを入力不可にする（手順１３１７）。

【００７２】以上の処理によって生成される画面の一例が、図２３中の検査パラメータ領域である。図２２，図２３では、「ＧＵＩ格納ディレクトリ名」が入力不可の領域となっている。また、図２４に、手順ノード選択時の検査パラメータ領域を生成する一例を示す。また、図２５に、検査実行手段のノード選択時の検査パラメータ領域を生成する一例を示す。

【００７３】図に示すように、手順パラメータは、検査手順に属する検査実行手段すべてを実行するために必要とされる実行パラメータのリストである。手順パラメータは、検査実行手段の情報に含まれる実行パラメータリスト（図１６に一例を示している）の和集合をとることによって生成される。また、検査実行手段のノードが選択された場合は、図２５に示すように、検査実行手段に対応づけられた検査実行手段の情報に含まれる実行パラメータリストのみを入力可能にする、または、デフォルト値を表示する。

【００７４】最後に、検査実行結果を他の検査の入力パラメータのデフォルト値とする処理について、図２６，図２７を参照しながら説明する。本実施の形態では、検査結果は成功、失敗の他に、取得されたデータとして、（データ名、データ型、値）を１エントリとするリストを返す。１５０１で検査を実行後、操作装置は検査実行装置から検査結果Ｒ（以下、「検査結果Ｒ」を「Ｒ」という）を取得する（手順１５０２）。

【００７５】次に、実行した検査の属する手順ノードの次のノードに関連付けられた手順データＤの手順パラメータリストに、Ｒに含まれるデータ名と同名の名前を持ったパラメータのエントリが存在するかどうかを確認する。もしも存在したならば、そのパラメータのデフォルト値としてＲ中の該当するデータを設定する（手順１５０６～１５１２）。

【００７６】上記処理を実行した検査の所属する手順ノード以降の全ての手順ノードに対して適用することで、検査実行結果を他の検査の入力パラメータのデフォルト値とすることができる（手順１５０４）。

【００７７】本実施の形態で示されるシステムにより、次のような特徴を持ったセキュリティホール診断ツールを実現することができる。

【００７８】まず、第１に、分類に使用する検査実行手段情報の属性名（分類キー名）と手順実行順序を手順定義として与え、実行時の検査項目を分類することで、知識の無い使用者でも、一般的な攻撃手順に即した順序で個々の検査を実行できるという特徴がある。

【００７９】更に、検査項目の各実行状態に応じて手順表示領域中のノードの表示を変化させることで、使用者が、現在検査がどこまで行われているのか、どの検査が成功し、また、失敗したのかに関して視覚的に把握することを可能にするという特徴がある。

【００８０】更に、各検査実行手段、及び検査手順で必要とされるパラメータの入力画面を動的に生成することで、検査実行手段の追加・削除・変更に柔軟に対応できるという特徴がある。検査実行手段の追加・削除・変更は、検査実行前に検査実行手段格納部５０４に格納され

た検査実行手段を編集することによって行う。

【００８１】更に、検査実行手段の実行結果により得られるデータを、（データ名、データ型、値）を１エントリとするリストで表現することで、検査実行手段の出力するデータを柔軟に設定できるという特徴がある。

【００８２】更に、上記特徴の形式で取得された検査結果のデータを、それ以降の検査の入力パラメータのデフォルト値として自動的に設定することで、使用者の入力作業を軽減することができるという特徴がある。

【００８３】実施の形態２．上記実施の形態１では、操作装置に３種類の画面を示したが、これに限られるわけではない。このセキュリティホール診断方式は、手順定義ファイルを編集する画面を備える場合であってもよい。この場合、予め、基本的な検査手順を表示し、表示された検査手順を利用者が編集する画面を提供する。

【００８４】例えば、次のような変更を実行する画面を提供する。

（１）検査名に対応する検査実行手段を変更（追加、削除）する。

（２）検査手順の検査の順番を変更する。

（３）検査名に対応する複数の検査実行手段を実行する順番を変更する。

上記以外の変更作業であっても構わない。

【００８５】また、複数の検査実行手段それぞれに対応する検査実行手段の情報（検査実行情報）に含まれる実行パラメータのデフォルト値、または、実行パラメータの項目を変更する画面を提供することも可能である。

【００８６】

【発明の効果】この発明に係るセキュリティホール診断方式によれば、検査実行手段に関する詳細な知識のないものでも、検査を実行することができる。

【００８７】このセキュリティホール診断方式の操作画面によれば、セキュリティホール診断に必要な検査手順の基本的な手順を把握することができる。

【００８８】このセキュリティホール診断方式の操作画面によれば、手順に対応する検査実行手段を把握することができる。

【００８９】このセキュリティホール診断方式の操作画面によれば、手順を実行するために必要な実行パラメータを把握することができる。

【００９０】このセキュリティホール診断方式の操作画面によれば、入力が必要となる実行パラメータを知り、操作制御部によって、必要なパラメータを入力することができる。

【００９１】このセキュリティホール診断方式の操作画面によれば、各検査名に対応する検査実行手段を実行する順番を把握することができる。

【００９２】このセキュリティホール診断方式の操作画面によれば、検査名に対応する手順パラメータ（実行パラメータの和集合）を把握することができる。

【００９３】このセキュリティホール診断方式の操作画面によれば、検査実行手段に必要な実行パラメータを把握することができる。

【００９４】このセキュリティホール診断方式の操作画面によれば、検査対象装置から検査結果を取得し、取得した検査結果を用いて、次の検査実行手段を実行することができる。

【００９５】このセキュリティホール診断方式によれば、検査結果を表示することができる。

【図面の簡単な説明】

【図１】　実施の形態１のセキュリティホール診断方式のシステム全体の一例を示す図。

【図２】　実施の形態１の検査実行装置の構成の一例を示す図。

【図３】　実施の形態１の操作装置の構成の一例を示す図。

【図４】　実施の形態１の手順定義ファイルの書式の一例を示す図。

【図５】　実施の形態１の表示名定義ファイルの書式の一例を示す図。

【図６】　実施の形態１の操作装置のに表示される主画面（操作画面）の構成の一例を示す図。

【図７】　実施の形態１の操作装置に表示される対象ホスト情報入力画面の構成の一例を示す図。

【図８】　実施の形態１の操作装置に表示される検査結果表示画面の構成の一例を示す図。

【図９】　実施の形態１の操作装置に表示される主画面の検査実行手段の実行情報を示すマークの一例を示す図。

【図１０】　検査実行手段の分類手順（情報読み込み段階）の動作の一例を示すフロー図。

【図１１】　初期化時における検査手順情報の初期化手順（手順パラメータ生成段階）の動作の一例を示すフロー図。

【図１２】　手順表示領域４０１における初期画面構築手順（画面表示段階）の動作の一例を示すフロー図。

【図１３】　手順定義ファイルの内容を説明する図。

【図１４】　検査実行手段の情報を説明する図。

【図１５】　検査実行手段の情報をプロパティ名”ＰＬＵＧＩＮ＿ＴＹＰＥ”で検策する場合を説明する図。

【図１６】　検査実行手段の情報の実行パラメータリストを説明する図。

【図１７】　主画面の手順表示領域で利用者が手順ノードを選択した場合の手順パラメータ領域生成の動作の一例を示す図。

【図１８】　主画面の手順表示領域で利用者が手順ノードを選択した場合の手順パラメータ領域生成の動作の一例を示す図。

【図１９】　主画面の手順表示領域で利用者が手順ノードを選択した場合に生成された手順パラメータ領域の一

例を示す図。

【図２０】　主画面の手順表示領域で利用者が検査実行手段のノードを選択した場合の手順パラメータ領域生成の動作の一例を示す図。

【図２１】　主画面の手順表示領域で利用者が検査実行手段のノードを選択した場合の手順パラメータ領域生成の動作の一例を示す図。

【図２２】　主画面の手順表示領域で利用者が検査実行手段のノードを選択した場合に生成された手順パラメータ領域（実行パラメータ設定前）の一例を示す図。

【図２３】　主画面の手順表示領域で利用者が検査実行手段のノードを選択した場合に生成された手順パラメータ領域（実行パラメータ設定後）の一例を示す図。

【図２４】　主画面の手順表示領域で利用者が手順ノードを選択した場合の検査パラメータ領域の手順パラメータを説明する図。

【図２５】　主画面の手順表示領域で利用者が検査実行手段のノードを選択した場合の検査パラメータ領域の実行パラメータを説明する図。

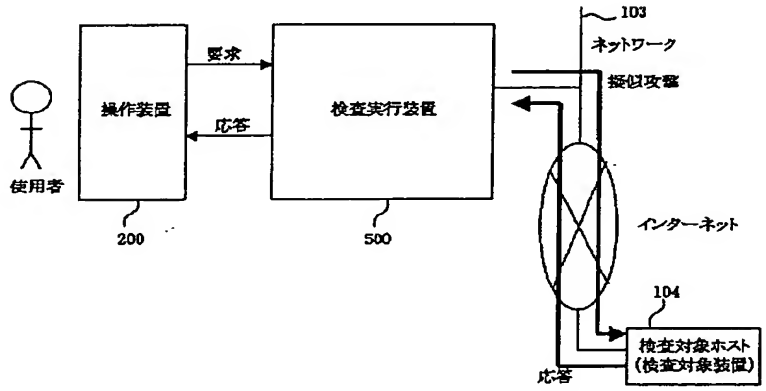
【図２６】　一の検査実行手段の検査結果を次の検査に再利用するための動作の一例を示す図。

【図２７】　一の検査実行手段の検査結果を次の検査に再利用するための動作の一例を示す図。

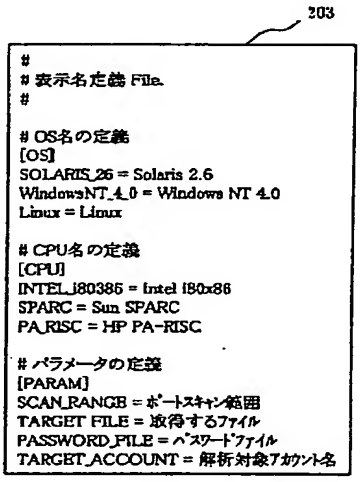
【符号の説明】

１０３　ネットワーク、１０４　検査対象ホスト、２００　操作装置、２０１画面生成部、２０２　手順定義ファイル、２０３　表示名定義ファイル、２０４　操作制御部、２０５　ディスプレイ、３０１　主画面（操作画面）、３０２対象ホスト情報入力画面、３０３　検査結果表示画面、４０１　手順表示領域、４０２　検査パラメータ領域、５００　検査実行装置、５０１　実行制御部、５０２　対象ホスト情報格納部、５０３　検査実行手段、５０４　検査実行手段格納部、９０１～９０４　検査の実行状況を表すマーク。

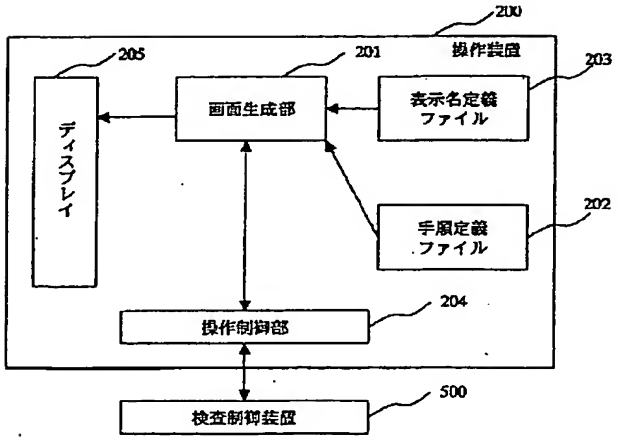
【図１】



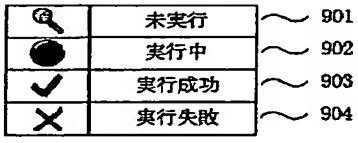
【図５】



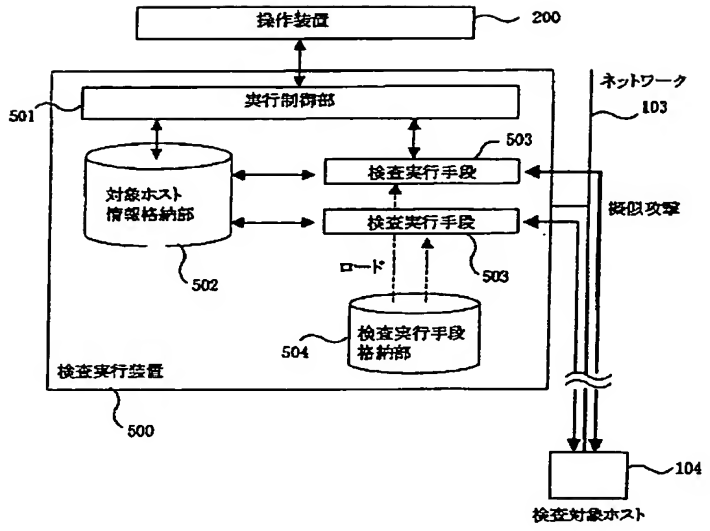
【図３】



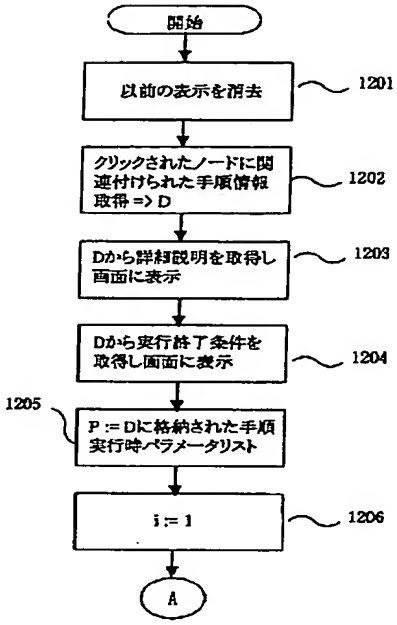
【図９】



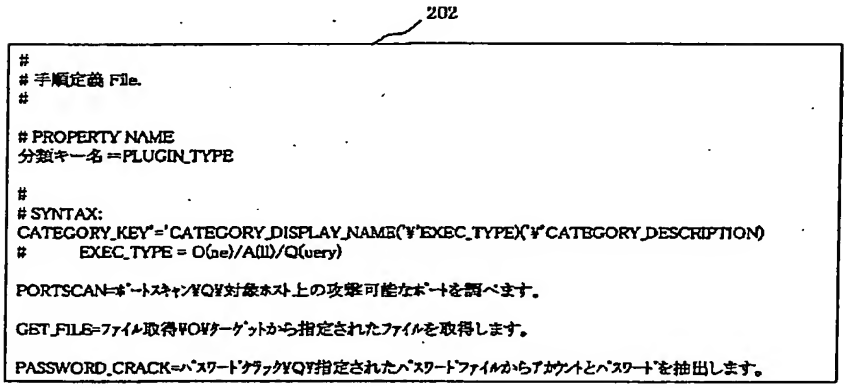
【図２】



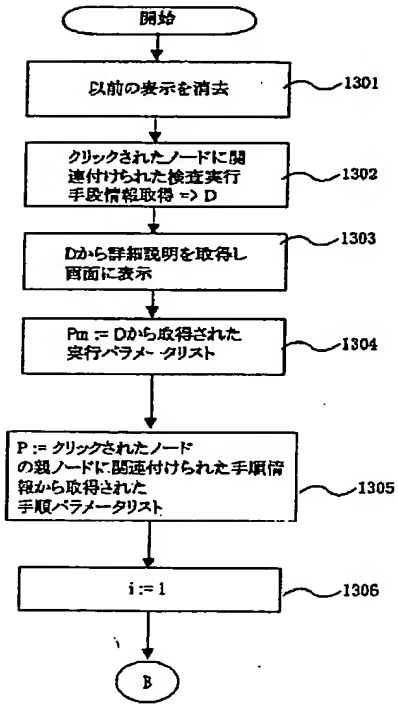
【図１７】



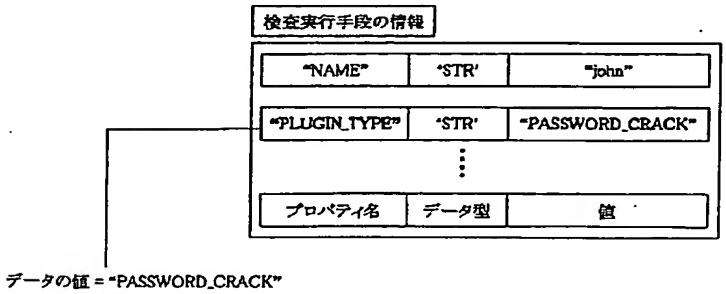
【図４】



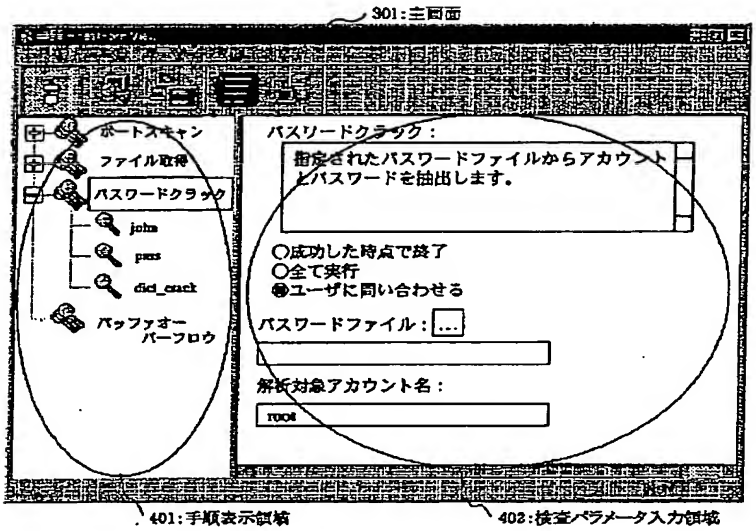
【図２０】



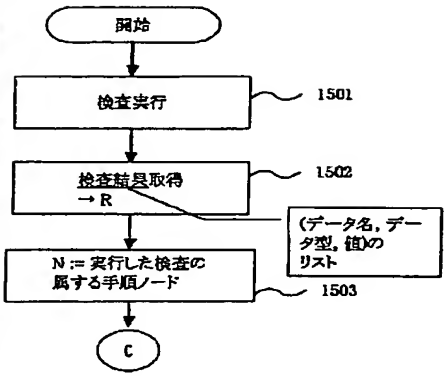
【図１５】



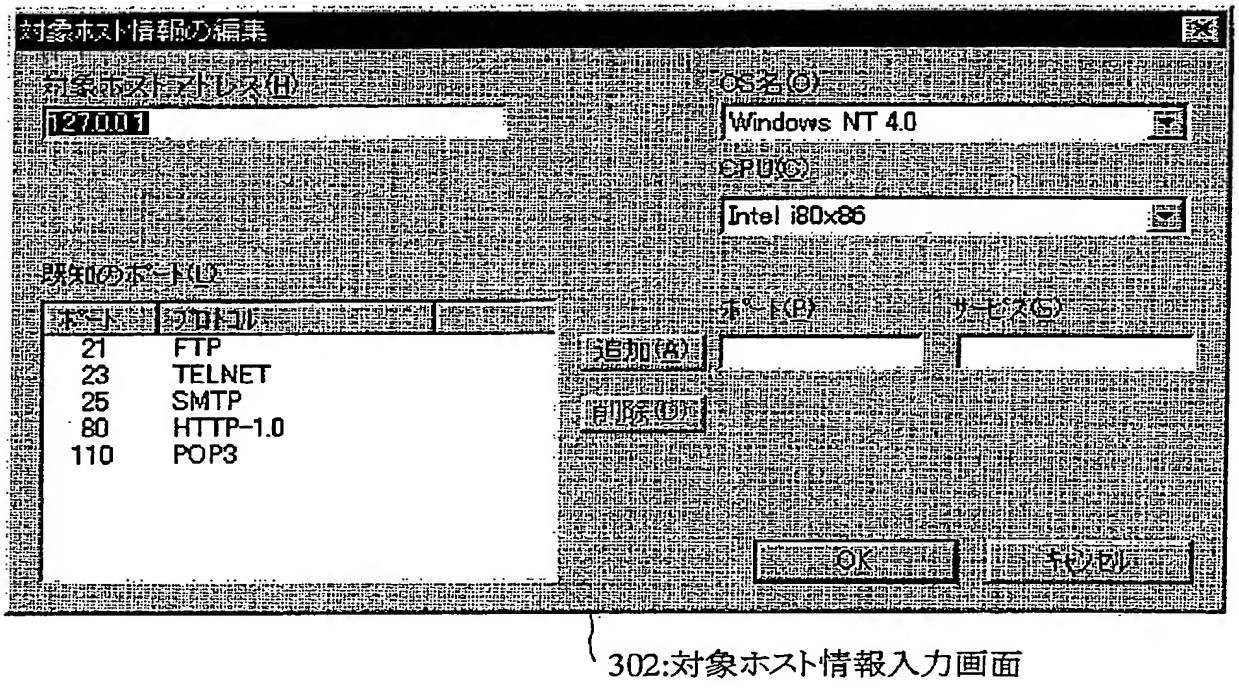
【図６】


301:主画面
ポートスキャン
ファイル取得
パスワードクラック
john
pass
did_crack
バッファオーバーフロウ
パスワードクラック：
指定されたパスワードファイルからアカウントとパスワードを抽出します。
○成功した時点で終了
○全て実行
◉ユーザに問い合わせる
パスワードファイル：
解析対象アカウント名：
root
401:手順表示領域
402:検査パラメータ入力領域

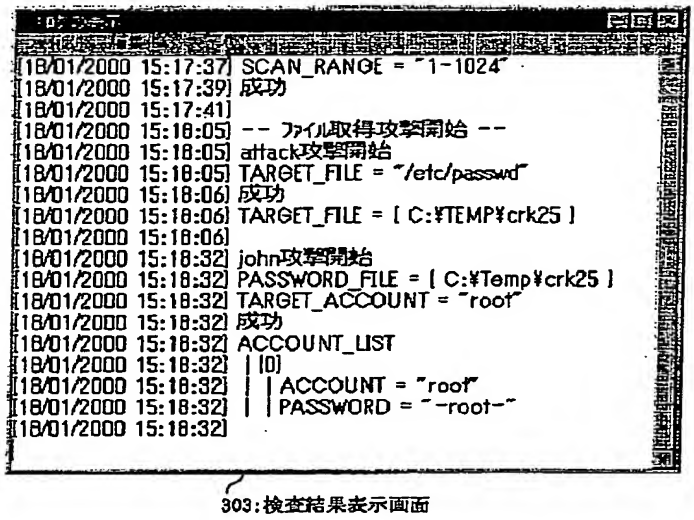
【図２６】


開始
検査実行
1501
検査結果取得
→R
1502
(データ名，データ型，値)のリスト
N := 実行した検査の属する手順ノード
1503
C

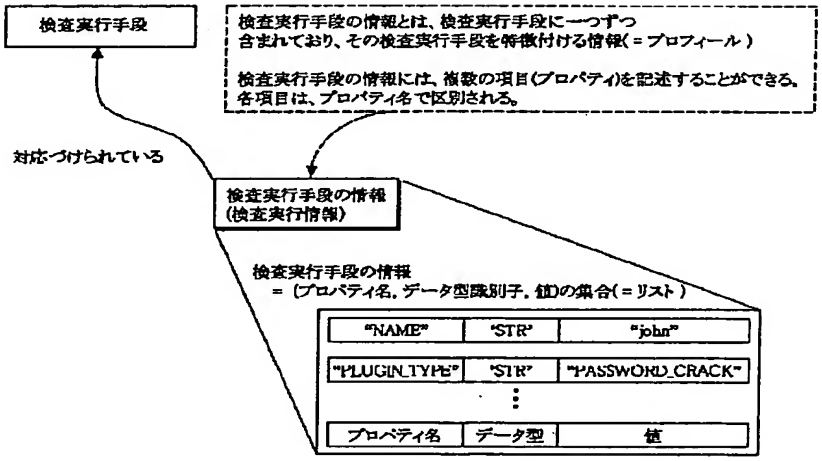
【図７】


対象ホスト情報の編集
対象ホストアドレス(H)
127.0.0.1
OS名(O)
Windows NT 4.0
CPU(C)
Intel i80x86
既知のポート(L)
ポート
プロトコル
21 FTP
23 TELNET
25 SMTP
80 HTTP-1.0
110 POP3
追加(A)
削除(D)
ポート(P)
サービス(S)
OK
キャンセル
302:対象ホスト情報入力画面

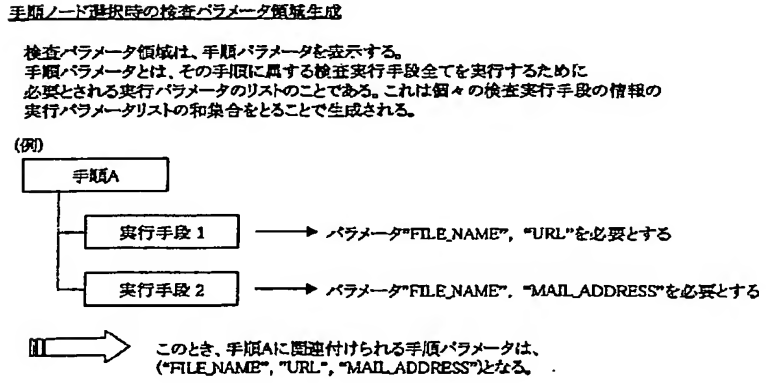
【図８】


[18/01/2000 15:17:37] SCAN_RANGE = "1-1024"
[18/01/2000 15:17:39] 成功
[18/01/2000 15:17:41]
[18/01/2000 15:18:05] -- ファイル取得攻撃開始 --
[18/01/2000 15:18:05] attack攻撃開始
[18/01/2000 15:18:05] TARGET_FILE = "/etc/passwd"
[18/01/2000 15:18:06] 成功
[18/01/2000 15:18:06] TARGET_FILE = [C:¥TEMP¥crk25]
[18/01/2000 15:18:06]
[18/01/2000 15:18:32] john攻撃開始
[18/01/2000 15:18:32] PASSWORD_FILE = [C:¥Temp¥crk25]
[18/01/2000 15:18:32] TARGET_ACCOUNT = "root"
[18/01/2000 15:18:32] 成功
[18/01/2000 15:18:32] ACCOUNT_LIST
[18/01/2000 15:18:32] | [0]
[18/01/2000 15:18:32] | | ACCOUNT = "root"
[18/01/2000 15:18:32] | | PASSWORD = "-root-"
[18/01/2000 15:18:32]
303:検査結果表示画面

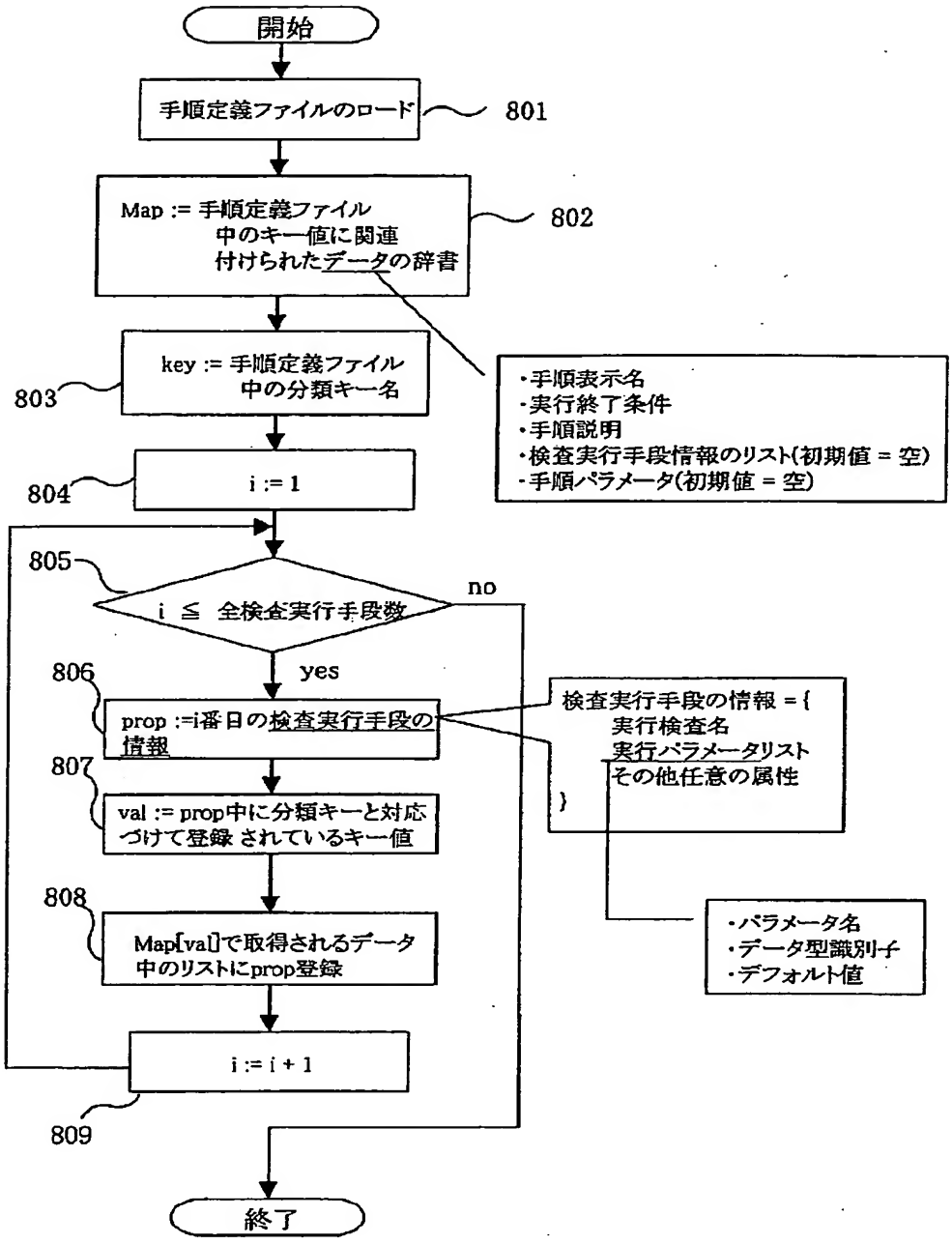
【図１４】


検査実行手段
検査実行手段の情報とは、検査実行手段に一つずつ
含まれており、その検査実行手段を特徴付ける情報(= プロフィール)
検査実行手段の情報には、複数の項目(プロパティ)を記述することができる。
各項目は、プロパティ名で区別される。
対応づけられている
検査実行手段の情報
(検査実行情報)
検査実行手段の情報
= (プロパティ名, データ型識別子, 値)の集合(= リスト)
"NAME"
"STR"
"john"
"PLUGIN_TYPE"
"STR"
"PASSWORD_CRACK"
プロパティ名
データ型
値

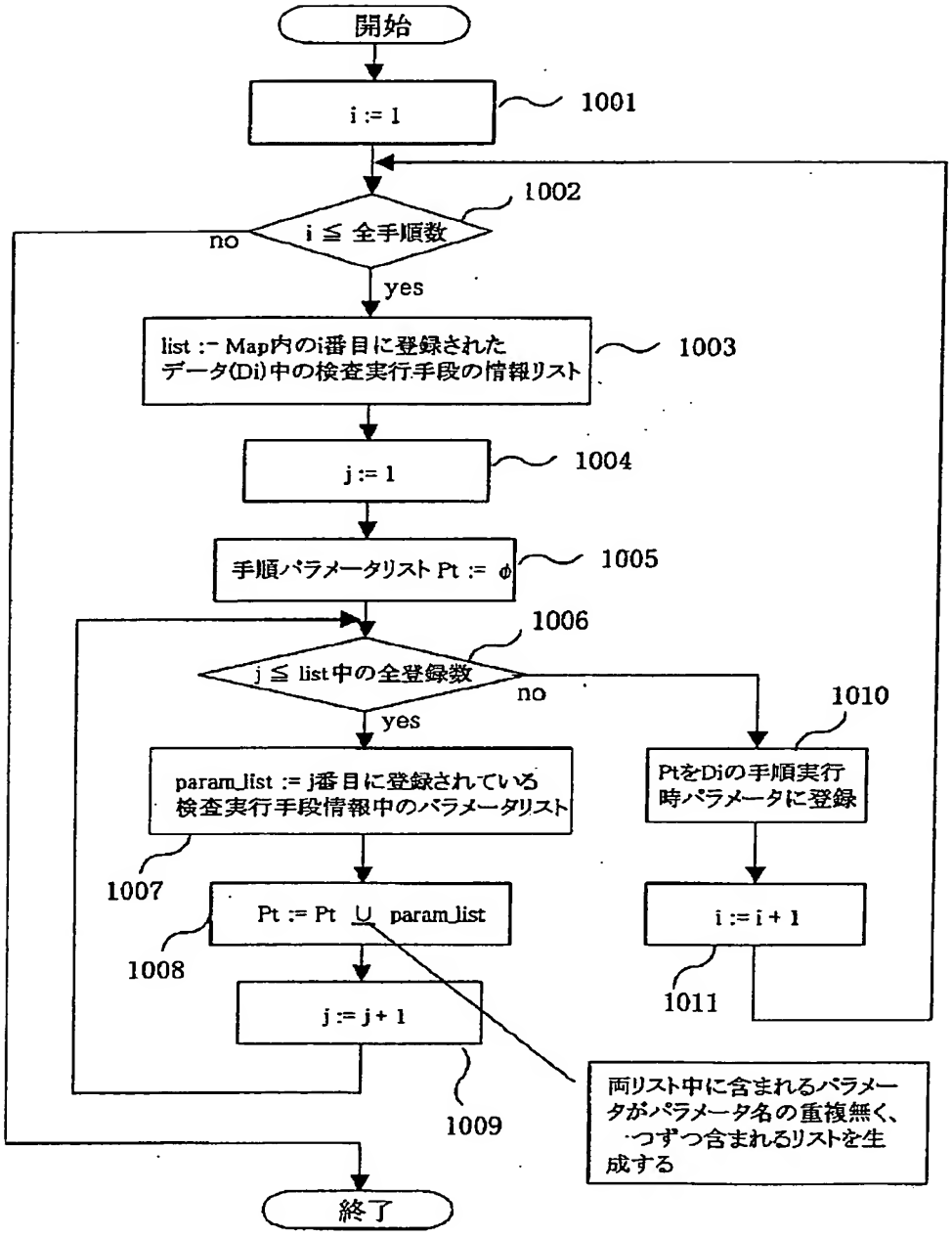
【図２４】


手順ノード選択時の検査パラメータ領域生成
検査パラメータ領域は、手順パラメータを表示する。
手順パラメータとは、その手順に属する検査実行手段全てを実行するために
必要とされる実行パラメータのリストのことである。これは個々の検査実行手段の情報の
実行パラメータリストの和集合をとることで生成される。
(例)
手順A
実行手段 1
パラメータ"FILE_NAME", "URL"を必要とする
実行手段 2
パラメータ"FILE_NAME", "MAIL_ADDRESS"を必要とする
このとき、手順Aに関連付けられる手順パラメータは、
("FILE_NAME", "URL", "MAIL_ADDRESS")となる。

【図１０】


開始
手順定義ファイルのロード
801
Map := 手順定義ファイル
中のキー値に関連
付けられたデータの辞書
802
・手順表示名
・実行終了条件
・手順説明
・検査実行手段情報のリスト(初期値 = 空)
・手順パラメータ(初期値 = 空)
key := 手順定義ファイル
中の分類キー名
803
i := 1
804
805
i ≦ 全検査実行手段数
no
yes
806
prop :=i番目の検査実行手段の
情報
検査実行手段の情報 = {
実行検査名
実行パラメータリスト
その他任意の属性
}
807
val := prop中に分類キーと対応
づけて登録 されているキー値
808
Map[val]で取得されるデータ
中のリストにprop登録
・パラメータ名
・データ型識別子
・デフォルト値
i := i + 1
809
終了

【図１１】


開始
i := 1
1001
1002
i ≦ 全手順数
no
yes
list :- Map内のi番目に登録された
データ(Di)中の検査実行手段の情報リスト
1003
j := 1
1004
手順パラメータリスト Pt := φ
1005
1006
j ≦ list中の全登録数
no
yes
1010
param_list := j番目に登録されている
検査実行手段情報中のパラメータリスト
PtをDiの手順実行
時パラメータに登録
1007
Pt := Pt ∪ param_list
i := i + 1
1008
1011
j := j + 1
1009
両リスト中に含まれるパラメータがパラメータ名の重複無く、一つずつ含まれるリストを生成する
終了

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.